Metodik för säkra tekniska system i teknikutvecklingens framkant

STPA (Systemteoretisk Processanalys)

Framtida tekniska system med en ökad grad av autonomi är för komplexa för kompletta systemsäkerhetsanalyser, men samtidigt för organiserade för att betrakta som slumpmässiga.

Detta medför ett antal utmaningar för att säkerställa att systemen erbjuder betryggande säkerhet. Dessa utmaningar behöver mötas med en metodik som kan hantera hög grad av systemkomplexitet. Systemteoretisk processanalys (STPA) är en analysmetod som baseras på en sådan metodik, vilken kan stödja arbetet med att säkerställa att även tekniska system i teknikutvecklingens framkant blir säkra.

Utmaningar vid systemsäkerhetsarbete för komplexa system

- Traditionella analysmetoder sträcker sig till att hantera komponentfel. För komplexa tekniska system är kompletta analyser av komponenter inte möjligt.
- Analysmetoder behöver hantera det dynamiska system av interaktioner mellan komponenter som avsiktligt eller oavsiktligt kan uppstå i autonoma och mycket komplexa system (exv. system med programvara).
- Konstruktion av säkerhetskritiska system ska beakta människors förutsättningar och begränsningar. För säkra system krävs därför hantering av Human factors integration, användbarhet och utformning av användargränssnitt.

Vad är Systemteoretisk processanalys?

STPA är en metod för riskanalys baserad på systemteori som tillämpas alltmer internationellt för att hantera autonoma system.

Utöver komponentfel antas med STPA att olyckor också kan orsakas av komponenters beteenden och inbördes interaktioner samt att ett system kan vara farligt trots att alla delarna uppfyller givna specifikationer, exempelvis att kravställningen har brister.

Utökad modell för hantering av olycksrisker

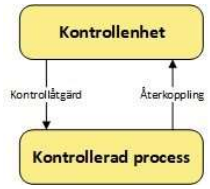
För komplexa system är en olycksriskmodell med linjära orsakssamband, med fokus på komponentfel, inte tillräcklig för att hantera de komplexa orsakssamband som kan leda till olyckor.

Inom STPA betraktas systemsäkerhet istället som ett dynamiskt kontrollproblem. Med detta avses att olyckor uppstår då de systembeteenden och anpassningar som är nödvändiga för att upprätthålla säkerheten brister. Detta kan exempelvis bero på brister i övervakningen av ett systems beteende eller fel i modellen för vilken som är korrekt åtgärd vid ett visst givet tillfälle.

För att förutse hur olyckor skulle kunna uppstå tillämpas en abstrakt kontrollmodell för att beskriva samband för det tekniska systemet.

Kontrollmodellen används vid konstruktion för att skapa nödvändiga kontrollåtgärder för systemet.

Med kontrollmodellen utvärderas även hur brister i kontroll av systemet kan medföra olyckor.



En kontrollenhet i modellen ovan skulle exempelvis kunna vara en programvara eller människa som tar beslut baserat på återkoppling från den kontrollerade processen.

Exempel
En självbromsande bil ska bevaka omgivningen och själv styra över bromsfunktionen, dvs. när och med vilken kraft en inbromsning ska göras.

Följande är exempel på osäkra kontrollåtgärder som kan genomföras av bromsfunktionen:

- Utebliven inbromsning.
- Bromsning leder till fara, exv. inbromsning vid fel tillfälle.
- Bromsning görs, men för tidigt eller för sent.
- Bromsning görs för länge eller bromsning upphör för tidigt.

Vad tänker du? Vilka skulle effekterna på systemnivå kunna bli - vilka olyckor skulle kunna inträffa?

Styrkan med STPA-analysen är abstraktion. Riskanalysen görs på den abstrakta kontrollstrukturen, inte på den fysiska modellen av systemet. STPA-processen är iterativ för att succesivt skapa en utökad detaljeringsgrad för systemets kontrollstrukturer, men startar med väldigt enkla modeller, exempelvis genom blockschema.

Med STPA så möjliggörs att identifiera händelseförlopp och scenarion som är svåra att identifiera med traditionella analysmetoder. Detta kan exv. handla om programvaras roll för osäkra systemhändelser eller att olyckor kan uppstå på grund av felaktig kravställning, dvs. när ingenting har fallerat eller gått sönder.

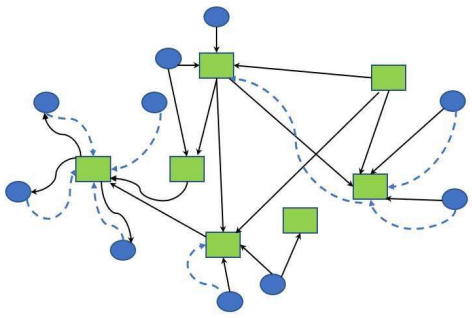
Utkomst av en STPA-analys
- Tydliggörande av vad som krävs av komponenterna i den föreslagna systemarkitekturen för att skapa och upprätthålla systemsäkerheten. Detta bidrar då konkret till kravdefinitionen för systemet och dess ingående delar.

- Utvärdera befintliga konstruktionsbeslut och identifiera brister och behov av förändring. Föreslå konstruktionsförändringar med avseende på systemsäkerhet.

- Identifiera och definiera testfall och testplaner för systemsäkerhetsinriktad verifiering.

STPA kan:

- Identifiera olycksrisker innan konstruktionen finns och kan därmed användas i kravhanteringen.
- Hantera mycket komplexa samband i autonoma system.
- Identifiera brister relaterade till användbarhet och mänskligt felhandlande.



Bakgrund till detta material
FMV har tagit fram detta mycket översiktliga material för att sprida information kring STPA (systemteoretisk processanalys).

FMV förordar denna metodik för autonoma och komplexa system i teknikutvecklingens framkant.

För mer information:
STPA Handbook 2018

Frågor: systemsakerhet.fmv@fmv.se