Slutrapport för projekt 2015-04840, SoSSE1

Säkerhetsutvärdering för system-av-system, förstudie

Författare: Jakob Axelsson och Avenir Kobetski, SICS Swedish ICT
Datum: 2016-08-15
Delprogram: Elektronik, mjukvara och kommunikation

FFI Fordonsstrategisk Forskning och Innovation
VINNOVA Energimyndigheten TRAFIKVERKET
FKG VOLVO SCANIA VOLVO

Innehållsförteckning

1 Sammanfattning 3

2 Executive summary 3

3 Bakgrund 4

4 Syfte, frågeställningar och metod 4

5 Mål 5

6 Resultat och måluppfyllelse 6

7 Spridning och publicering 6

7.1 Kunskaps- och resultatspridning 7

7.2 Publikationer 7

8 Slutsatser och fortsatt forskning 7

9 Deltagande parter och kontaktpersoner 8

10 Referenser 9

Kort om FFI

FFI är ett samarbete mellan staten och fordonsindustrin om att gemensamt finansiera forsknings-, innovations- och utvecklingsaktiviteter med fokus på områdena Klimat & Miljö samt Säkerhet. Satsningen innebär verksamhet för ca 1 miljard kr per år varav de offentliga medlen utgör drygt 400 Mkr.

För närvarande finns fem delprogram; Energi & miljö, Trafiksäkerhet och automatiserade fordon, Elektronik, mjukvara och kommunikation, Hållbar produktion och Effektiva och uppkopplade transportsystem. Läs mer på www.vinnova.se/ffi

1 Sammanfattning

Framtida lösningar inom kooperativa intelligenta transportsystem (C-ITS) kommer i allt större utsträckning innebära att autonoma eller halvautonoma fordon sammankopplas till system-av-system (SoS). De olika ingående delarna, både fordon och infrastruktur, kommer behålla ett visst oberoende, både vad gäller dess drift och ägarskap, och detta innebär nya utmaningar för säkerhetsanalysen. Dagens metoder, såsom ISO 26262, är helt inriktade på att säkerställa att en systemleverantör (t ex en OEM) kan garantera den egna produktens säkerhet. Detta räcker dock inte för att uppnå säkerhet i det sammankopplade SoS, då den övergripande säkerheten är en funktion av det dynamiska samspelet mellan de ingående delarna.

Detta projekt var en förstudie med syfte att pröva nya metoder för säkerhetsanalys baserade på systemtänkande, för att lösa problemen som uppstår i SoS. Projektet utförde en säkerhetsanalys för konvojkörning av lastbilar, s k platooning, för att bättre förstå vilka tekniker som är lämpliga för C-ITS. I ett planerat huvudprojekt kommer sedan dessa resultat att vidareutvecklas och generaliseras för att täcka ett bredare spektrum av SoS.

Huvudsökande för projektet var SICS Swedish ICT, och övrig part var AB Volvo. Projektet pågick från november 2015 till juni 2016. Den totala budgeten var 1,2 MSEK, varav 0,6 MSEK utgjordes av offentliga medel.

2 Executive summary

Future solutions within the field of cooperative intelligent transportations systems (C-ITS) will increasingly require autonomous or semi-autonomous vehicles interconnecting into systems-of-systems (SoS). The constituent parts, both vehicles and infrastructure, will generally maintain a certain independence, both with respect to operation management and ownership. This poses new challenges to the safety analysis. Current safety methods, such as ISO 26262, are focused on each system supplier (e.g. an OEM) analyzing its own products safety. However, this is not sufficient to guarantee the overall safety of an interconnected SoS, since it is highly dependent of the dynamic interaction of the constituent systems.

This report describes a pre-study project, with the aim of learning and trying out new methods for safety analysis of SoS, based on systems thinking. The project carried out a safety analysis of a C-ITS applications, consisting of several vehicles driving in a platoon formation close behind each other and autonomously controlling their speed so as as to follow the leader vehicle at a close distance.

The safety analysis method that was studied in detail is called *STAMP* or *Systems Theoretic Accident Model and Processes* (Leveson, 2011). It is heavily founded in systems theory and always considers a system in its entirety, including not only the technical system, but also human operators, policy makers, software, etc. Specifically, *STECA* (*Systems Theoretic Early Concept Analysis*) (Fleming, 2016), a STAMP-variation that is suitable for analysing systems at early development stages was used, together with the more widespread causal analysis workflow of the STAMP framework, named STPA (*System Theoretic Process Analysis)*.

The results of this pre-study are promising, indicating that STAMP may indeed be a suitable method for the safety analysis of SoS applications. Not only does it allow to consider systems in its entirety, but it is also hierarchic by its nature, and allows to zoom in and out on interesting portions of a systems or a SoS. This also allows to rather easily update the safety analysis if a part of a SoS is suddenly updated or exchanged. The explicit focus of STECA on systems that are far from the final development stage is also very suitable for SoS application, which are expected to be rather volatile.

While the conclusion is that STAMP is promising for analyzing SoS safety, a number of challenges still remain. One such challenge is the different ownership of the SoS constituents. In general, STECA assumes that there exists some sort of concept of intended system operation. This might be more difficult to achieve in the SoS case and

needs further investigation. Also, the speed of change that SoS might experience, as well as their scale may be a challenge.

Another practical issue is the integration of the STAMP method into existing safety practices and standards, such as for example ISO 26262. This project has touched upon the issue and there is good hope that these methods can in fact be integrated successfully. However, of course, this should be proven.

In summary, this project has scratched the surface and showed some promising results for the application of STAMP to SoS. However, to reach practical maturity, deeper and broader studies are needed, both in terms of method development and the scale and variety of SoS applicaitons.

3 Bakgrund

System-av-system (engelska system-of-systems, eller SoS), är en term som används för att beskriva system som är sammansatta av flera oberoende ingående system, som samarbetar för att uppnå ett gemensamt syfte (Maier, 1998). Dessa SoS utmärks av att:

- De ingående systemen drivs oberoende, vilket innebär att de har en meningsfull existens även utanför ett SoS.
- De ingående systemen förvaltas oberoende, vilket innebär att de har olika ägare.
- Evolutionär utveckling, där de olika ingående systemen vidareutvecklas utan att samordnas sinsemellan, och där strukturen på SoS kan ändras över tiden.
- Emergent, eller framträdande, beteende är själva syftet med att skapa SoS, man vill uppnå en funktion som ingen av delarna ensam kan uppnå.

SoS som begrepp har funnits i några decennier, men har främst studerats för militära tillämpningar (Axelsson, 2015a). I samband med digitaliseringen av samhället har dock relevansen ökat även för andra branscher, genom att man numera allt oftare vill koppla samman system för att effektivisera informationsflöden och automatisera arbetsprocesser.

För att kartlägga åtgärdsbehoven kring SoS i Sverige har nyligen en omfattande kartläggning gjorts, av en stor grupp industriella och offentliga aktörer, vars resultat presenteras i en forsknings- och innovationsagenda för området (Axelsson, 2015b). Agendans övergripande slutsats är att Sverige behöver skaffa sig en världsledande förmåga att snabbt utveckla trovärdiga SoS. Trovärdigheten är viktig för att kunna använda tekniken även för kritiska tillämpningar, t ex i transportsektorn, och i detta begrepp är säkerhet en av nyckeldelarna.

Inom fordonssektorn bedrivs sedan ett antal år tillbaka utveckling av s k kooperativa ITS-system (C-ITS), och dessa utgör utmärkta exempel på SoS. Syftet med C-ITS är att fordon, deras förare, infrastrukturen och väghållare ska samarbeta för att uppnå säkrare, effektivare och behagligare resor. En grundsten i detta är kommunikation mellan fordon, och med infrastruktur vid vägsidan.

4 Syfte, frågeställningar och metod

En viktig fråga som är relativt obehandlad är hur man ska uppnå säkerhet i C-ITS-system, där ett fordon blir beroende av information från andra. Här kan kunskap från SoS-området bidra, men man har varken i forskning eller industrin sammankopplat kunskapen inom SoS med C-ITS. Syftet med detta projekt är att inleda ett utforskande av metoder för säkerhetsanalys av C-ITS, och den övergripande forskningsfrågan blir därför:

Hur kan man utföra säkerhetsanalys av SoS, med tillämpning inom C-ITS?

Arbetet har grundat sig i hypotesen att säkerhetsanalyser baserade på systemtänkande krävs, och detta motiveras av att orsaken att skapa ett SoS är att man vill uppnå ett emergent beteende, vilket alltså inte kan

analyseras fullt ut genom ett reduktionistiskt synsätt där man betraktar de enskilda delarna utan hänsyn till det dynamiska samspelet mellan dem.

Då projektet är att betrakta som en inledande förstudie så har fokus lagts på att explorativt undersöka en tillämpning, nämligen konvojkörning av lastbilar, för att därigenom skapa en fördjupad förståelse för hur säkerhetsanalysen bör bedrivas. I ett större uppföljningsprojekt planeras detta att utvidgas och generaliseras till både fler C-ITS-funktioner, och till andra SoS, samt en utökad validering av metoderna.

Säkerhetsanalys är ett område med en lång tradition av forskning, och många av resultaten har sedan paketerats i standarder som beskriver ”best practice”, t ex ISO 26262 som är förhärskande i fordonsindustrin. Dessa standarder utmärks dock av att de tittar på en begränsad del av det totala SoS, och på senare tid har mycket kritik riktats mot detta synsätt (Rasmussen, 1997). Man hävdar istället att man måste se säkerheten i ett systemperspektiv, där man tittar både på tekniska lösningar, människan i loopen, och även t ex organisatoriska och legala strukturer. Detta angreppssätt verkar lämpa sig väl för SoS såsom C-ITS, och därför har en modern version (Leveson, 2011) av detta synsätt använts som ett teoretiskt ramverk för projektet. Detta ramverk kallas *STAMP (Systems Theoretic Accident Model and Processes)* och har utvecklats vid MIT. En viktig utgångspunkt i detta är att mjukvaran utgör en allt viktigare del i moderna produkter, och skiljer sig från andra komponenter genom att de inte går sönder i klassisk mening, t.ex. genom utmattning. Detta gör att traditionella säkerhetsanalyser som utgår från en händelsekedja som börjar med att en komponent fallerar, och slutar med en olycka, är svåra att tillämpa. Ramverket tar också hänsyn till det faktum att många olyckor inte beror på en enstaka komponent, utan är ett resultat av komplexa interaktioner mellan många delar, vilket också är utmärkande för SoS. Säkerhet är helt enkelt en emergent egenskap som uppstår om komponenterna interagerar med varandra på rätt sätt. STAMP försöker därför identifiera kontrollfunktioner som strävar efter att styra systemets beteende mot säkra områden, s k ”safety envelops”.

5 Mål

Både forskning och konkret utveckling bedrivs sedan ett antal år tillbaka inom C-ITS-området. Fokus har legat på att uppnå förbättrad bränsleförbrukning, utveckla regleralgoritmer, samt konstruera kommunikationsprotokoll. Allt detta är viktiga delar, med hög relevans för FFI-programmet, och de förväntade värdena som C-ITS ska skapa är väl dokumenterade.

Dock har mindre vikt hittills lagts vid att utreda hur C-ITS-tekniken ska bli tillräckligt säker. Detta är naturligtvis en förutsättning för att tekniken ska kunna sättas i drift i stor skala, vilket innebär att de önskade fördelarna inte kommer att kunna realiseras om inte metoder för säkerhetsanalys tas fram. Detta projekt tar viktiga steg i denna riktning, och är därför en möjliggörare för att kunna uppnå de vinster som man önskar vad gäller energiförbrukning, transporteffektivitet och trafiksäkerhet. Ett antal av delprogrammen förutsätter att C-ITS ska bidra till att uppfylla deras mål, och förutsätter därmed också indirekt att tillräcklig säkerhet kan nås, men utan att beskriva hur detta ska gå till. Konkret anges följande i de olika delprogrammen:

- Inom energi och miljö anges konvojkörning som ett viktigt sätt att minska bränsleförbrukning, och ger enligt tidningen Scania World möjligheter att nå 15% förbättring.
- Inom trafiksäkerhet och automation ses konvojkörning som ett viktigt steg på vägen mot automatiserad körning, och man beskriver hur det interaktiva fordonet kan bidra till ökad säkerhet.
- Inom elektronik, mjukvara och kommunikation identifierar man funktionell säkerhet och systemsäkerhet som en viktig del inom området autonoma fordon, och man talar även om fordon-till-fordons-kommunikation (V2V) som en möjliggörare för autonom körning.
- Inom effektiva och uppkopplade transportsystem innefattar både milsten 2 och 3 i färdplanen konvojkörning.

Projektet har således bäring på många delprogram, och vi har valt att ansöka inom elektronik, mjukvara och kommunikation, eftersom det är inom detta område som säkerhetsanalys ges störst vikt.

Projektet är ett samarbete mellan akademin, i form av forskningsinstitutet SICS Swedish ICT som är en del av RISE, och industrin, i form av AB Volvo. Denna typ av samarbeten är också prioriterade inom FFI. Resultaten är i förlängningen tillämpbara även på andra typer av säkerhetskritiska SoS, vilket ger en potential för branschöverskridande samverkan.

6 Resultat och måluppfyllelse

Projektet var uppbyggt kring fem heldags workshoptillfällen, då deltagare från de båda projektparterna träffades och diskuterade såväl uppnådda resultat som aktuella frågeställningar.

Efter en inledande konkretisering av en exempelapplikation av C-ITS påbörjades arbetet med den interna kompetensuppbyggnaden. Dels var det viktigt att få en klar bild för statusen på tekniken för konvojkörning samt vilka utmaningar och möjligheter den erbjuder i dagsläget. Och dels var det viktigt att bättre förstå lämpligheten av existerande säkerhetsanalysmetoder för SoS-applikationer. I gränslandet mellan dessa två områden ligger den egentliga forskningsfrågan för detta projekt, nämligen hur man ska analysera säkerheten i C-ITS, eller mer generellt i SoS. En systematisk litteraturstudie gjordes över vetenskapliga publikationer inom ”safety” (säkerhet) och ”platooning” (konvojkörning), som resulterade i en tidskriftspublikation (se nedan). En slutsats av den studien var att metodiken för säkerhetsanalys ligger en bra bit efter den tekniska utvecklingen inom C-ITS-området. I de (publicerade) fall som säkerhetsanalys överhuvudtaget har utförts var det ofta av antingen översiktlig eller begränsad karaktär, isolerad till antingen enstaka säkerhetsrisker eller tekniska komponenter.

Därefter gjordes en genomgripande analys av en C-ITS-applikation med hjälp av den systemteoretiska säkerhetsanalysmetoden STAMP. Som en bas för detta tillbringade Axelsson och Kobetski en vecka på MIT för att fördjupa kunskapen om metoden. Applikationen studerades i sin helhet, bestående bl.a. av lastbilar, förare, mjukvara, kommunikationsutrustning och en central trafikplanerare. Målet var att visa på hur STAMP skulle kunna appliceras på C-ITS samt detektera eventuella brister i STAMP vid hantering av SoS. En viktig slutsats är att för halvautomatiserad körning, såsom konvojer, är samspelet mellan teknik och människa en central frågeställning, och STAMP tar hänsyn till denna aspekt i större utsträckning än många etablerade analysmetoder. En annan frågeställning som är viktig för C-ITS är datasäkerhet, genom att man öppnar upp fordonen för extern kommunikation, och datasäkerhet och fysisk säkerhet kommer att hänga samman mer än de tidigare gjort. Även här finns möjligheter att utöka STAMP för att ta hänsyn till datasäkerhet och samspelet med fysisk säkerhet.

Förutom kunskapsuppbyggnaden, som var ett av projektets delmål, har arbetet med STAMP-metodiken visat på lovande resultat för att analysera säkerheten i SoS tillämpningar, vilket uppfyller projektet andra delmål. En vidare formalisering och utvidgning av STAMP-metodiken, samt dess anpassning till de rådande arbetssätten inom fordonsindustrin är dock, inte helt oväntat, fortsatt öppna frågor.

Ett av förstudiens mål var att ta fram en projektansökan för ett huvudprojekt. Under förstudien påbörjades arbetet med en större ansökan inom platooning (Sweden 4 Platooning), och där ligger en fördjupad säkerhetsanalys för denna applikation med som en del. Därutöver finns tankar om att fortsätta arbetet med säkerhetsanalyser för mer generella system-av-system, där man tittar på fler applikationer inom transportområdet, men kanske också inom andra domäner. Detta arbete kommer att fortsätta under hösten 2016.

7 Spridning och publicering

Syftet med detta projekt var främst att undersöka möjligheterna till mer djupgående studier samt att bygga upp den interna kompetensen inom den studerade frågan hos de ingående parterna. Trots att fokuset därmed inte har legat på den externa publiceringen, har arbetet lett till ett par publikationer.

7.1 Kunskaps- och resultatspridning

Hur har/planeras projektresultatet att användas och spridas?	Markera med X	Kommentar
Öka kunskapen inom området	X	Detta har varit en av grundpelarna för projektet och har uppfyllts.
Föras vidare till andra avancerade tekniska utvecklingsprojekt	X	En tänkt fortsättning på projektet har inkluderats i ett större samarbete mellan bl.a. flera lastbilstillverkare, vars mål är att få till en fungerande prototyp av konvojkörning. Ansökan för det nya projektet är inlämnad, men beslutet är ännu inte taget.
Föras vidare till produktutvecklingsprojekt	-	För tidigt.
Introduceras på marknaden	-	För tidigt.
Användas i utredningar/regelverk/ tillståndsärenden/ politiska beslut	-	Även om det inte finns några planer på detta just nu, skulle den studerade metoden kunna passa mycket väl till sådana utredningar.

7.2 Publikationer

Följande publikationer har författats under projektets gång:

- En litteraturstudie inom säkerhet för konvojkörning har blivit accepterad till tidskriften IEEE Transactions on ITS (Axelsson, 2016). Detta är en mycket ansedd tidskrift, som rankas på första plats inom transportområdet i söktjänsten Google Scholar.
- En konferensartikel som beskriver projektet har accepterats till en svensk workshop om system-av-system (Kobetski, 2016), och kommer att presenteras i september 2016.
- Denna konferensartikel kommer att utvidgas och skickas till en internationell konferens under hösten 2016, med troligt presentationsdatum under våren 2017.
- Dessutom har en kortare populärvetenskaplig artikel skrivits under arbetet med projektansökan (Axelsson, 2015c), men innan själva projektet startades. Den beskriver problemställningen och ansatsen.

Därutöver har olika arbetsmaterial och en teknisk slutrapport sammanställts och delats inom projektkonsortiet.

8 Slutsatser och fortsatt forskning

En tydlig slutsats är att STAMP, med sitt tydligt systemorienterade förhållningssätt, är på många sätt en lämplig metod för analys av SoS. Dock finns det ett antal fortsatta utmaningar. SoS anses vara snabbt föränderliga system, i ständig utveckling, där man kanske inte ens fullt ut vet hur SoS-funktionaliteten kommer att bete sig vid tiden för design och utveckling av det individuella systemet. Detta är något som en säkerhetsanalysmetod måsta ta höjd för. Den bör vara flexibel, snabbt uppdaterbar, och kunna ta hänsyn till otydliga specifikationer. STAMP visade sig vara en kraftfull metod vad gäller uppdaterbarheten, tack vare sin hierarkiska natur. En del av STAMP-ramverket, med namnet *Systems Theoretic Early Concept Analysis (STECA)*, har tillämpats på C-ITS-applikationen och visat sig vara lovande när det gäller hanteringen av just otydliga eller ofärdiga specifikationer. Dock är det fortfarande oklart hur den kommer att skala med SoS där olika system ägs och tillverkas av olika aktörer.

En del arbete lades även ner på att jämföra STAMP med det inarbetade sättet att analysera säkerheten av enskilda komponenter inom fordonsindustring, nämligen ISO 26262. En slutsats här är att båda metoderna

har mycket att erbjuda, men på olika sätt. Medan ISO 26262 tillhandahåller ett standardiserat ramverk för säkerhetsrelaterade frågor under hela utvecklings- och livscykeln av ett fordon, är STAMP mer fokuserad på själva kärnan inom säkerhetsanalysen. Det känns troligt att dessa två ramverk kan giftas ihop på ett fördelaktigt sätt, där man fortsätter att använda sig av ISO 26262's inarbetade arbetsprocesser och standarder, samtidigt som själva riskanalysdelen ersätts av STAMP's angreppssätt, med dess helhetsperspektiv på system och risker. Medan det känns som en intressant väg framåt återstår utmaningen att få ihop dessa ramverk på ett bra sätt, inte minst när det kommer till ISO 26262's ASIL-säkerhetsklassning.

Sammanfattningsvis har projektet resulterat dels i en kunskapsuppbyggnad och genomgång av forskningsläget inom säkerhetsanalys av C-ITS, och dels i en verklig applikation av en systemteoretisk metod för säkerhetsanalys till ett exempel på C-ITS-applikation. Projektet har bekräftat bilden av att forskningen inom säkerhetsanalys av komplexa system har varit eftersatt och har lyckats skrapa på ytan över de utmaningar och möjligheter vi idag står inför inom detta område. På det viset har målen för detta förstudieprojekt uppnåtts. För att C-ITS- eller SoS-tillämpningar ska kunna bli verklighet krävs det dock att man gräver djupare och bredare, d.v.s. både inom metodutveckling och storleken på de analyserade systemen, för att komma ikapp den tekniska utvecklingen inom dessa områden.

9 Deltagande parter och kontaktpersoner

Huvudsökande för projektet var SICS Swedish ICT, och övrig part var AB Volvo. Från SICS Swedish ICT's sida deltog Jakob Axelsson och Avenir Kobetski i arbetet. AB Volvo bidrog med kunskap och diskussioner från ett antal olika personer med olika kompetenser, med Katrin Sjöberg i rollen som samordnare.

10 Referenser

Axelsson, J. (2015a). A Systematic Mapping of the Research Literature on System-of-Systems Engineering. In IEEE 10th Annual System of Systems Engineering Conference.

Axelsson, J. (2015b). Systems-of-systems for border-crossing innovation in the digitized society - A strategic research and innovation agenda for Sweden.

Axelsson, J. (2015c). Safety Analysis for Systems-of-Systems. ERCIM News (102). pp. 22-23. ISSN 0926-4981.

Axelsson, J. (2016). Safety in Vehicle Platooning: A Systematic Literature Review. To appear in IEEE Transactions on Intelligent Transportation Systems. doi: 10.1109/TITS.2016.2598873

Fleming, C., Leveson, N. (2016), Early Concept Development and Safety Analysis of Future Transportation Systems. To appear in IEEE Transactions on Intelligent Transportation Systems. doi: 10.1109/TITS.2016.2561409

Kobetski, A., Axelsson, J. (2016). System-based Safety Analysis of Automotive SoS Applications. To appear in Proc. 2 nd Swedish Workshop on the Engineering of Systems of Systems (SWESoS).

Leveson, N. (2011). Engineering a Safer World: Systems Thinking Applied to Safety. Retrieved from https://books.google.com/books?hl=sv&lr=&id=0gZ_7n5p8MQC&pgis=1
8Version på projektbeskrivningsmall 2013-06-17

Maier, M. W. (1998). Architecting principles for systems-of-systems. Systems Engineering, 1(4), 267–284. doi:10.1002/(SICI)1520-6858(1998)1:4<267::AID-SYS3>3.0.CO;2-D

Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. Safety Science. Elsevier Sci B.V.