Final Report

HoliSec (Holistiskt angreppssätt att förbättra datasäkerhet)

Publik rapport

Version:	V1.0
Projektakronym:	HoliSec
Vinnova Diarie Nr:	2015-06894
Projektledare:	Lars-Olof Berntsson
Författare:	Daniel Kåberger
Datum:	2019-10-01

FFI Fordonsstrategisk Forskning och Innovation

VINNOVA Energimyndigheten TRAFIKVERKET FKG VOLVO SCANIA VOLVO

Innehållsförteckning

Kort om FFI
FFI är ett samarbete mellan staten och fordonsindustrin om att gemensamt finansiera forsknings- och innovationsaktviteter med fokus på områdena Klimat & Miljö samt Trafiksäkerhet. 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

Tillkomsten av autonoma och anslutna fordon har skapat nya utmaningar för bilindustrin som ställer krav på att fordon ska utformas för att förbli pålitliga även vid förekomsten av cybersäkerhetsattacker. Nya UNECE-förordningar kommer att kräva bevis på att fordonet skall vara utformat för att vara motståndskraftigt mot attacker som kan påverka datasäkerheten, och att fordonet skall vara utformat med förmågan att upptäcka dessa attacker och svara på lämpligt sätt.

Vinnova/FFI projektet HoliSec[1] koordinerades av Volvo Technology AB och fokuserade på datasäkerhet för system i fordon i en föränderlig miljö.

HoliSec har genererat resultat inom :
• arkitektur och arkitekturdesignprinciper(t.ex..Secure On Board Communication och Secure Diagnostics),
• metoder och verktyg för Threat Analysis Risk Assessment (TARA),
• hur förebygga och upptäcka attacker (t.ex. IDS),
• samspel mellan funktions- och data-säkerhet.

Projektpartners i HoliSec projektet var ArcCore, Assured, Chalmers, RISE Research Institutes of Sweden, Volvo Car Group och Volvo Technology AB (VTEC). Projektets varaktighet blev tre och ett halvt år, med projektstart 2016. Budgeten var 40,6 MSEK, varav 20,3 MSEK offentliga medel.

2 Executive summary in English

The advent of autonomous and connected vehicles has created new challenges for the automotive industry that require vehicles to be designed to remain reliable in the presence of attacks that can affect data security. New UNECE regulations will require proof that the vehicle is designed to be resistant to attacks that may affect data security, and that the vehicle should be capable of detecting and responding appropriately.

The Vinnova/FFI HoliSec project [1] was coordinated by Volvo Technology AB and focused on data security for systems in vehicles in a changing environment.

HoliSec[1] has generated results in:

• architecture and architecture design principles (e.g. Secure On-Board Communication and Secure Diagnostics),

• methods and tools for Threat Analysis Risk Assessments (TARA),

• how to prevent and detect attacks (e.g. IDS),

• interaction between functional safety and data security.

Project partners in the HoliSec project [1] were ArcCore, Assured, Chalmers, RISE Research Institutes of Sweden, Volvo Car Group, and Volvo Technology AB (VTEC). The duration of the project was three and a half years, with project start in 2016. The budget was 40.6 MSEK, of which 20.3 MSEK was public funding.

3 Bakgrund

Fordonssystem kommer alltid vara ett mål för hackare varför förmågan att utveckla fordon med datasäkerhet som en del i utformningen är av största vikt. Vi behöver utforma fordonen på ett sådant sätt att de kan motstå skadliga attacker. Tidigare forskningsprojekt, så som projektet HEAVENS [2] samt pågående arbete med framtagning av ISO21434 [3] (kommande ISO standard för cybersäkerhet i vägfordon), har lagt grunden för detta och har definierat metoder för hur hot- och riskanalyser (TARA) bör utföras på ett strukturerat sätt. Dessa metoder följer en traditionell riskbaserad säkerhetsutformningsprocess (livscykel) för fordon så som de som är definierade i ISO 26262 [4] (ISO standard för funktionssäkerhet i vägfordon).

Relaterade forskningsprojekt har fokuserat på utformningen av säkra fordonssystem, givet att en riskanalys har genomförts. Säker referensarkitektur har utvecklats i HEAVENS- [2] och EVITA [6]-projekten. Referensarkitekturer handleder designers i hur man utformar en strukturerad och säker design.

För att vidareutveckla och komplettera forskningen runt datasäkerheten i uppkopplade fordon så genomfördes framgångsrikt, under tre och ett halvt år, projektet HoliSec [1] som fokuserade på att producera användbara resultat för fordonsindustrin. Driftsatta resultat har gjort att både personbilar och lastbilar blivit säkrare genom att öka medvetenheten för hur potentiella hot kan, och skall, bemötas med teknologier och nödvändiga säkerhetskomponenter.

4 Syfte, forskningsfrågor och metod

4.1 Syfte

När projektet initierades 2015 såg vi att det inom bilindustrin var ett paradigmskifte mot självkörande och uppkopplade fordon. Marknadsundersökningar 2015 förutspådde att 85% av alla bilar skulle vara uppkoppplade till internet redan år 2020 och cyber-relaterade brott skulle vara ett riktigt hot för industrin.

Redan 2015 var bilden klar att fordon inte bara skulle kunna kommunicera mellan varandra för att lösa kritiska trafiksituationer, utan fordonsägarna, förare och passagerare skulle även få tillgång till ytterligare funktionalitet och bli en del av ”Internet of Things” (IoT).

Det var också tydligt att integration av nya och mera avancerade teknologier skulle medföra nya risker. Det var därför nödvändigt att investera i forskning och utveckling så att säkerhets- och integritetsproblem inte hindrade utvecklingen av dessa nya funktioner. I annat fall förutsågs att detta kunde ha en direkt påverkan på trafiksäkerheten för både nya och befintliga marknader inom fordonsindustrin.

Att kunna garantera fordonssäkerhet och kunna utveckla framtida nya funktioner är ett krav och det är allmänt känt att fordonstillverkare som misslyckas med att tillgodose ny funktionalitet på ett säkert sätt kommer vara väldigt sårbara i framtiden. Det är inte osannolikt att en eller flera tillverkare kommer vara utlåsta från vissa marknader, eller till och med försvinna helt på grund av stora säkerhets- och integritetsproblem.

Säkerhet och integritet kan inte längre hanteras som isolerade teknologier eller läggas till i efterhand i systemutvecklingsprocessen. Snarare behöver säkerhet och integritet vara integrerade i processen redan från systemets utformning. Syftet med HoliSec [1] har därför varit att öka medvetenheten hur potentiella hot kan och skall bemötas med teknologi och nödvändiga säkerhetskomponenter, samt addressera hela kedjan från koncept, design, produktutveckling, integration mot tredje-partsprodukter, val av tekniska lösningar till testning, validering och verifiering samt operationella faser.

4.2 Forskningsfrågor

Hur kan säkerhet och integritet bli integrerade i processen redan från systemets utformning där hela kedjan adresseras från koncept, design, produktutveckling, integration mot tredje-parts produkter, val av tekniska lösningar till testning, validering och verifiering samt operationella faser? Kan projektet försöka påverka och utveckla gemensamma **krav**, **bästa praxis, riktlinjer** och **ramverk** för den svenska fordonsindustrin? [**Obj2**, **Obj4**]

Hur kan identifierade säkerhetskrav bli synliga genom hela kedjan och påverka samtliga beslut rörande utformningen? Eftersom fordon behöver kunna hantera inte bara aktuella hot, utan även nya hot som uppstår de kommande 10 till 20 åren, finns det ett stort behov av att inte bara kunna detektera utan också med kort varsel hantera och lösa säkerhetsproblem. Samtliga säkerhetslösningar utvecklade idag behöver vara flexibla nog att möjliggöra framtida utbyggnad och förändring för att vara fullt användbara i en förändringsbar hotmiljö. [**Obj1**]

Projektet har ställt frågor runt hur man utformar med datasäkerhet och integritet i åtanke, hur komponenter integreras i fordon på ett sådant sätt att säkerhetsproblem inte kan påverka fordonets säkerhet. [**Obj1, Obj3**]

Passagerarbilar, bussar och lastbilar använder för närvarande olika teknologier och har olika tekniska begränsningar. Det finns därför en vinning i att sprida framtagna tekniker och metoder som kan användas inom flera domänområden inom fordonsindustrin. [**Obj2, Obj5, Obj6**]

4.3 Metod

Med ett holistiskt synsätt, alltså genom att titta brett över flera områden och teknologier rörande datasäkerhet inom fordonsindustrin och försöka lära oss, har HoliSec [1] samarbetat inom forskning på olika områden, personbilsidan, lastbilssidan, och strävat att bygga kompetens inom olika områden, samt att kombinera akademiska forskningspartners med OEMer inblandade i både passagerarfordon, bussar och lastbilar. Medverkande företag ifrån två olika typer av OEMer har varit viktigt eftersom passagerarbilar och kommersiella fordon (som bussar och lastbilar) för närvarande inom vissa områden använder olika teknologier och har olika tekniska begränsningar. Denna möjlighet att samarbeta mellan OEMer och forskningspartners är tämligen unik och vi anser att det har förbättrat kostnadseffektiviteten och ökat den internationella konkurrenskraften.

För att kunna genomföra samarbetet mellan de olika OEMerna och de akademiska partners inblandade i projektet så delades projektet upp i ett antal arbetspaket. Varje arbetspaket har sedan belyst olika datasäkerhetsrelaterade områden och tekniker. Partners har sedan jobbat med att bedriva forskning och undersökningar i de olika arbetspaketen. Ett övergripande fokus har varit att sprida medvetenheten runt datasäkerhet inom fordonsindustrin .

Översikt över arbetspaketen:

- [WP 0] – Projektledning
- [WP 1] – Säkerhets- och integritetskrav vid anslutning av fordon
- [WP 2] – Kryptografiskt stöd och nyckelhantering
- [WP 3] – Säkerhetsmekanismer för uppkopplade fordon
- [WP 4] – Säker utveckling och styrning
- [WP 5] – Demonstration och spridning

5 Mål

5.1 Mål som redogjordes vid projektansökan

Datasäkerhet och integritet kan inte längre hanteras som isolerade teknologier eller som en eftertanke i systemutvecklingsprocessen. Snarare behöver datasäkerhet och integritet vara integrerade i processen redan i systemets initiala utformning. I HoliSec-projektet [1] tog vi upp dessa frågor genom ett **holistiskt angreppssätt**. Vi adresserade hela kedjan från koncept, design, produktutveckling, integration mot tredje-parts produkter, val av tekniska lösningar till testning, validering och verifiering samt till operationella faser. Det övergripande målet var att försöka påverka och utveckla gemensamma **krav**, **bästa praxis, riktlinjer** och **ramverk** för den svenska fordonsindustrin. [**Obj2**, **Obj4**]

Det var viktigt att identifierade säkerhetskrav var synliga genom hela kedjan och att dessa krav påverkar samtliga beslut rörande utformningen. Eftersom fordon behöver kunna hantera inte bara aktuella hot, utan också nya hot som uppstår de kommande 10 till 20 åren, fanns det ett stort behov av att inte bara kunna detektera, utan också med kort varsel hantera och lösa datasäkerhetsproblem. Samtliga datasäkerhetslösningar utvecklade idag behöver vara flexibla nog att möjliggöra framtida utbyggnad och förändring för att vara fullt användbara i en förändringsbar hotmiljö. Ett fordon som inte konstruerats för datasäkerhet kommer ha det svårt att hantera framtida hot som uppstår och denna typ av design kommer endast leda till reaktivt datasäkerhetsarbete vilket resulterar i ett konstant arbete med att åtgärda de senaste upptäckta problemen i datasäkerheten.[**Obj1**]

Design med datasäkerhet och integritet i åtanke

Vi fokuserade därför på hur man **utformar med datasäkerhet** och integritet i åtanke, hur **komponenter integreras** i fordon på ett sådant sätt att datasäkerhetsproblem kan påverka fordonets datasäkerhet. Vi undersökte olika typer av mekanismer som är användbara i implementering av datasäkerhetsfunktioner i fordon och utvecklade metoder och mekanismer för datasäkerhetstestning och för att tidigt få varningar vid intrångsdetektering. Dessa är nödvändiga komponenter för att kunna garantera fordonssäkerhet och fordonstillverkare som misslyckas med att tillgodose sådana funktionier kommer vara väldigt sårbara i framtiden. Det är inte osannolikt att en eller flera tillverkare kommer vara utlåsta från vissa marknader eller till och med försvinna helt på grund av stora datasäkerhets- och integritetsproblem. [**Obj1, Obj3**]

Enbart OEMer som har en sund datasäkerhetsutformning, som kan garantera fordonets datasäkerhet, och kan hantera problem med integriteten, kommer kunna erbjuda ny avancerad funktionalitet i framtiden, så som självkörande funktioner och fordon som tillåts medverka i V2X tjänster. OEMer som misslyckas att erbjuda sådan funktionalitet kommer att hålla sig bakom marknadsledare avseende funktioner och användbarhet. Vi strävade därför att bygga kompetens inom området genom att kombinera akademiska forskningspartners med OEMer inblandade i både passagerarfordon samt kommersiella fordon (bussar och lastbilar). Medverkande ifrån två olika typer av OEMer var viktigt eftersom passagerarbilar, bussar och lastbilar för närvarande inom vissa områden använder olika teknologier och har olika tekniska begränsningar. Denna möjlighet att samarbeta mellan OEMer och forskningspartners var tämligen unik och har förbättrat kostnadseffektivitet och ökat den internationella konkurrenskraften. [**Obj2, Obj5, Obj6**]

Samarbete på flera områden

Vi studerade och undersökte existerande säkerhetsrelevanta teknologier från olika industriella domäner, ex. IT, telekom, och processindustri, och om möjligt anpassa dem till kontexten för fordonsindustrin. Även om det är många unika komponenter i fordonsdomänen så är det möjligt att några av begränsningarna eller problemen är snarlika inom andra domäner, och att andra tillvägagångssätt eller tekniska lösningar kan användas. Domäner som undersöktes inkluderade andra transportdomäner så som flyg- och rymdindustrier, men också industriella kontrollsystem och ”smart-grid”-säkerhet var av intresse. Som en sidoeffekt har det också lett till att andra lösningar och teknologier utvecklade i detta projekt kunnat överföras till andra domäner.[**Obj3**]

5.2 Sammanfattning av mål

Mål	Vision och mål	Kortfattad motivering	Nivå
Specifika för FFI Fordonssäkerhet och Integritet			
Obj1	Förstå utmaningar med datasäkerhet och associerade datasäkerhets-, integritets-, finansiella, och operationella risker genom ett holistiskt synsätt.	HoliSec gav processer för att hjälpa till med säker utveckling, öka förståelsen för datasäkerhetskrav och risker, hela vägen från tidig utveckling till sent i testningsfaserna.	Hög
Obj2	Utveckla gemensamma bästa praxis, riktlinjer och regelverk för den svenska fordonsindustrin.	HoliSec assisterade den svenska fordonsindustrin genom utveckling av gemensamma processer/metoder/regelverk. Detta har möjliggjort en snabbare och mer effektiv utveckling samtidigt som det adresserat datasäkerhet genom enande arbete mellan svenska fordonstillverkare så väl som förenklat kommunikationen med leverantörer, kunder och myndigheter.	Hög
Obj3	Undersöka existerande datasäkerhetsrelevanta teknologier från andra industriella domäner och om möjligt anpassa dem till kontexten för fordonsindustrin. Om så krävs, undersöka och utveckla nya fordonsspecifika datasäkerhetsteknologier.	HoliSec undersökte, utvärderade och apassade relevanta metoder, säkerhetsmekanismer och verktyg som nu även används inom andra domäner inom kontexten för fordonsindustrin.	Hög
Obj4	Undersöka, utveckla och integrera processer för att säkerställa datasäkerhet.	Holisec utvecklade State-of-the-Art processer som ligger i linje med existerande säkerhetsstandarder, så som ISO 26262	Hög
Övergripande för FFI, inom områdena Klimat & Miljö och Säkerhet			
Obj5	Öka den svenska kapaciteten inom forskning och innovation och därigenom säkerställa konkurrenskraft och jobb inom fordonsindustrin.	Tillräcklig och effektiv hantering av datasäkerhetsproblem har ökat konkurrenskraften inom den svenska fordonsindustrin och gett åtkomst till marknader där lagstiftning ställer krav inom området för fordonsdatasäkerhet.	Hög
Obj6	• Utveckla internationellt sammankopplade och konkurrenskraftiga forsknings- och inovationsmiljöer i Sverige. • Främja små och medelstora företags deltagande. • Främja branschövergripande samarbete • Främja samarbete mellan industrier, forskningsinstitut, universitet och högskolor.	Holisec sammanförde flera svenska OEMer och leverantörer tillsammans med akademin och forskningsinstitut inom datasäkerhetsområdet för att hitta en gemensam vy över hur datasäkerhet kan bli integrerat i elektroniska fordonssystem och processer, såväl som hur en integrerad syn på datasäkerhet i E/E arkitektur utvecklas.	Hög

6 Resultat och måluppfyllelse

För att möta projektets mål har HoliSec [1] bland annat levererat resultat inom olika arbetsområden som beskrivs i mer detalj under respektive arbetsområde. Varje arbetsområde innehåller också den ursprungliga beskrivningen från projektstart, vad arbetsområdet förväntades innehålla eller inrikta sig på.

6.1 [WP 0] Projektledning

Innehåll
Projektledning och därmed förenlig verksamhet.

Konkreta Leveranser
Rapportering samt framgångsrik och effektiv projektledning som bidragit till goda resultat och leveranser från arbetspaketen.

Resultat
Projektledning har säkerställt god kvalitet i framtagna resultat som sedan nyttjats och spridits av de olika partners (även i samarbete med projektet DEX som publicerar information inom området på www.autosec.se), rapportering har skett på vederbörligt vis till Vinnova, regelbundna styrgrupps, ledningsgrupps- och projektmöten har hållits.

6.2 [WP 1] Säkerhets- och integritetskrav vid anslutning av fordon

Innehåll
Detta arbetspaket undersökte, ur ett datasäkerhets- och integritetsperspektiv, behoven och kraven för: (1) ökade nivåer av anslutning och automation i fordon, (2) åtkomstmetoder med både permanent och tillfällig åtkomst till fordonet och dess delar, och (3) delning av stora mängder data enligt användarens samtycke i samverkande ITS, prediktivt underhåll och produktförbättringar.

Arbetet omfattar redovisning av externa begränsningar så som förväntningar från kund och juridiska krav, så väl som OEM-begränsningar så som verksamhetskrav och ändrade arbetssätt (agil mjukvaruutveckling).

Projektet identifierade vad som var State-of-the-Art inom olika områden (e.x. metodiker och processer för säker design och verifiering, datasäkerhetsmekanismer, kryptering, standardisering), med tanke på den senaste forskningen inom fordons-domänen såväl som andra relevanta domäner, så som IT, telekom och processindustri.

Konkreta Leveranser
Leveransen av arbetspaketet [WP1] är direkt kopplad till resultatet som levererats genom hela HoliSec-projektet. Utöver det har också följande rapporter skapats som dokumenterar tidigare forskning inom området samt behov identifierade inom fordonsindustrin.

D1.1 Security & privacy for connected & automated vehicles
D1.2 A State-of-the-Art Report on Vehicular Security

Resultat
Behov och krav för datasäkerhet och integritet inom fordonsindustrin togs fram tidigt i projektet och kompletterades senare med mindre uppdateringar i MS2. Dessa behov och krav låg till grund för att definiera innehåll för respektive arbetspaket. Beskrivning av State-of-the-Art från projektet HEAVENS [2] utökades med beskrivningarna som omfattade HoliSecs utökade scope.

6.3 [WP 2] Kryptografiskt stöd och nyckelhantering

Innehåll
Detta arbetspaket undersökte lösningar för kryptering och nyckelhantering. Målet var att definera en livscykel för nyckelhantering och undersöka krypteringslösningar och algoritmer för nyckelhantering från andra domäner och deras tillämplighet på fordon.

Konkreta leveranser
Leverans av WP2 har skett genom att resultaten har dokumenterats i en rapport inom projektet och även publicerats i form av en vetenskaplig artikel på websidan www.autosec.se.

D2 Cryptographic Solutions for AUTOSAR Secure Onboard Communication

Resultat
Med utgångspunkt i att det via ODB-porten i fordon kan gå att koppla in okänd eller icke godkänd hårdvara i fordonet eller direkt till CAN-bussen, samt problematiken kring bristen på meddelandeintegritet på CAN-bussar, har ett förslag utformats för hur det är möjligt att skydda kommunikationen i CAN-nätverket. Förslaget omfattar användandet av AES-CTR för asymmetrisk kryptering för nyckelutbyte, symmetrisk kryptering för effektivt skydd av data, aggregerad autentisering av meddelanden genom MAC algoritm, samt nyckelderivering och nyckelfärskhet ("freshness"). Förslaget visar på möjlighet att säkra upp kommunikationen mellan komponenterna i nätverket och förhindra att okänd hårdvara kopplas in som manipulerar funktioner i fordonet.

6.4 [WP 3] Säkerhetsmekanismer för uppkopplade fordon

Innehåll
Detta arbetspaketet definierade mekanismer för att öka datasäkerhet i fordonssystem, med hänsyn till samspelet mellan datasäkerhet och integritet. Målet var att definiera riktlinjer för integration och användning av mekanismerna. I arbetet ingick även att utveckla och validera verktyg för testning av sådana mekanismer.

Uppgift 3.1 Säker fordonsdiagnostik (Ledare: Volvo Technology)
Metoder definierades för att upprätta förtroende mellan diagnostiskverktyg och ECUer (både trådade och trådlösa lösningar).

Uppgift 3.2 Säker kommunikation (Ledare: Chalmers)
Tillvägagångssätt undersöktes för att säkra fordonets kommunikationsnätverk (interna och externa). AUTOSAR-konceptet utvärderades för ”Secure On-Board Communication”.

Uppgift 3.3 Samspel mellan säkerhet och integritet (Ledare: SP)
Säkerhetsmekanismer definerades (hårdvara och mjukvara) och E/E arkitektur, med tanke på samspel mellan datasäkerhet och integritet. Metoder och verktyg tillämpades för att testa och utvärdera sådana datasäkerhetsmekanismer, både utifrån ett funktionssäkerhets- och datasäkerhetsperspektiv, med avseende på ISO 26262, AUTOSAR och testbarhet.

Uppgift 3.4 Loggning och intrångsdetektering (Ledare: VCC)
Lösningar definierades för loggning vid olika systemnivåer för att detektera intrångsförsök eller intrång.

Konkreta leveranser

Utöver nedanstående så har det också gjorts ett antal publiceringar inom området. Dessa är listade under *7.2 Publikationer.*

D3.1 Secure vehicle diagnostics
D3.2 Secure Communication
D3.3 Interplay between Safety, Security and Privacy
D3.4 Log and Intrusion Detection

Resultat

3.1. Under projektet utvecklades och presenterades en koncept-lösning för hur förtroende skapas mellan en diagnostiktestare och ECU:er. Resultatet av studien visar att det behöver upprättas en diagnostik-anslutning, mellan diagnostiktestaren och ECU:n, som bevarar äktheten hos användaren och diagnostik-testaren samt integriteten på data när det överförs. För att lösa detta föreslås en PKI-lösning.

3.2. Detta arbetet utvecklade säkerhetsprotokoll som definierats av AUTOSAR för ”on-board”-kommuniktion i syfte att uppfylla datasäkerhetskrav så som (1) Integritet, (2) Äkthet och att nyckelfärskhet (“freshness”) uppnås på kommunikationskanaler. Inledingsvis utvecklades en FVM (Freshness Value Manager), vars huvuduppgift är att hålla synkronisering mellan ECU:er (master och slav). Denna FVM används sedan tillsammans med modulen AUTOSAR SecOC för att säkra ”on-board”-kommunikation mellan master- och slav-ECU:er. Resultatet har demonstrerats genom att implementera säker kommunikation över CAN- och Ethernet-nätverk genom fyra scenarier, (a) Kommunikation över CAN-nätverk mellan två ECU:er (en master och en slav), (b) Kommunikation över CAN-nätverk mellan tre ECU:er (en master och två slavar), (c) Kommunikation över Ethernet-nätverk mellan två ECU:er (en master och en slav), (d) Kommunikation över Ethernet-nätverk mellan tre ECU:er (en master och två slavar). Efter varje implementation har tester genomförts för att utvärdera AUTSAR SecOC-modulen. Dessa inkluderar, (i) meddelandeförvanskning – kontrollera om slav-ECU detekterar att meddelandet blivit förvanskat, (ii) omsynkronisering – kontrollera att ECU omedelbart omsynkroniserar efter att den vaknat från ett sovande läge, (iii) prestandamätning – mäta lägsta latens på meddelandet mellan master och slav-ECU (med och utan säkerhet) med hänsyn till de krav som ställs på bromsljus-funktionalitet.

3.3. Samspelet mellan säkerhet och privacy har utretts genom en utvärdering av de vanligaste säkerhetsmekanismerna listade i ”IEC 62443”-standarden, projektet SESAMO, OWASP och NIST SP 800-53. Applicerbarheten av säkerhet och privacy har utretts genom att fokusera utvärderingen på attributen pålitlighet, säkerhet, underhållbarhet, tillgänglighet, integritet och konfidentialitet, men även på ytterligare säkerhetsattribut som definierats i säkerhetsmodellen från projektet HEAVENS, äkthet, auktorisation, oförnekbarhet, nyckelfärskhet (”freshness”) och integritet (privacy). Forskningen visade på att några av de studerade säkerhetsmekanismerna kan förbättra säkerhet och underhållbarhet medan enskilt användande av mekanismerna generellt ger lägre stöd för förbättring av systemets tillgänglighet och pålitlighet. I vissa fall hade säkerhetsmekanismer en negativ inverkan på säkerheten så som åtkomstkontroll där operatören kan bli utlåst vid kritiska events. Av 17 säkerhetsmekanismer som analyserats och baserat på de säkerhetsrelaterade attribut som berörs mest visade det sig att flest mekanismer har medium till hög positiv effekt på integritet (15 st), konfidentialitet (13 st) och auktorisering (13 st). Gällande privacy så är kryptering och virtuella privata nätverk (VPN) de som ger störst förbättring medan autentisering och signering har försumbar till ingen effekt på integritet. De flesta mekanismerna belyser intrångsdetektering men system för loggning, IDS, detektering av skadlig kod och operativsystem belyser intrångsdetektering i en större grad.

Vidare analyserades mekanismerna med hänsyn till implementationsnivå enligt ISO 26262 [4], användbarhet och resurskrav. Två mekanismer implementeras vanligtvis på hårdvara, fem mekanismer på mjukvarunivå och sju mekanismer på systemnivå med resterade tre som kan implementeras på antingen hård- eller mjukvarunivå.

En analys genomfördes över vilka säkerhetsmekanismer som kan användas för att mitigera olika hot, definierade av STRIDE-modellen, tillhörande cybersäkerhetsattacker och verktyg. Resultatet visar att varje hot definierat i STRIDE-modellen mitigeras med nästan hälften eller mer i de olika mekanismerna.

Slutligen genomförde studien också en utredning i hur mekanismerna kan testas i syfte att försäkra sig om att en viss säkerhetsnivå har uppfyllts. Utredningen visade på att de flesta av mekanismerna kan testas genom ett brett utbud av verktyg som listats i studien. Generellt kan också mekanismerna testas med de flesta testmetoderna. Vilket attackverktyg och vilken metod som används beror generellt på applikationen som skall testas samt dess hårdvaru-/mjukvarukonfiguration. [**Obj3]**

3.4. Forskningen som genomförts i arbetspaketet framhäver behov, utmaningar och krav för utveckling av intrångsdetekteringssystem (IDS) och loggning inom fordonsnätverk (In-Vehicle Networks, IVNs). Bidragen till området inom intrångsdetektering i fordon är trefaldigt. (a) En lättvikts IDS har uformats och implementets med en algoritm för en kombination av missbruk- och beteendedetektering. Den implementerade IDS:en kan detektera en basnivå av attacker så som en godtyckling injicering av meddelanden i nätverket samt attacker där egenskaper i meddelanden skiljer sig ifrån de ursprungliga specifikationerna. Detta har utvärderats på CAN-bussen i ett riktigt IVN. Arbetet förslår att övervakningen idealt skall ske genom en dedikerad ECU för varje IVN-domän. Dock på grund av hög produktionskostnad för en sådan lösning rekommenderas en gradvis integrering med prioritet på de mest kritiska domänerna.

(b) I det andra bidraget skapades en ny specifikations-agnostisk mekanik för detektering av attacker som överkommer begränsningarna i redan existerande arbete. Det snabba, lättviktiga och system-agnostiska tillvägagångsättet lär sig det normala beteendet hos IVN-dynamiken baserat på historiskt data och detekterar avvikelser genom att regelbundet övervaka IVN-trafiken.

(c) Som tredje bidrag har det implementerats en metod på enklare hårdvara och demonstrerats, genom utförliga experiment, inklusive att uföra attacker på en 2018 Volvo XC60 testbil, hur det till skillnad från existerande metoder var möjligt att detektera smygattacker på IVNs utöver de klassiska attackerna som existerar i litteratur. Gällande ämnet loggning visar utredningarna att säkerhetsevent som kan loggas är relativt begränsade i de flesta ECU:er. Även om mer avancerade ECU:er (e.x. infotainment-enheter) kan tillgodose stora möjligheter för loggning. Det har konstaterats att det är en viktig del av en stabil säkerhetshållning att spela in och samla säkerhetsevents eftersom det möjliggör incidentrespons som kan begränsa skada. **[Obj3] [Obj5] [Obj6]**

6.5 [WP 4] Säker utveckling och styrning

Innehåll

Arbetspaketet definierade metoder och tekniker för att närma sig datasäkerhet och integritet i fordonsmjukvara och system genom hela livscykeln för mjukvarautveckling.

Uppgift 4.1 Säker mjukvara och systemutformning (Ledare: Chalmers)

Med fokus på de tidigare faserna i livscykeln för säker mjukvaruutveckling (vänstra benet i ISO 26262 [4] Del 6 referensfasmodell för mjukvaruutveckling), krav, utformning, implementation, bygger detta arbetspaket på, samt utökande av, tidigare resultat från HEAVENS-projektet [2] inom samma område.

Uppgift 4.2 Säker validering och verifiering av mjukvara. (Ledare. SP)

Identifierade och utvecklade metoder och verktyg för validering och verifiering av säker mjukvaruutvecklings livscykel, snarlik och anpassad med ISO 26262 Del 6 [4].
Arbetspaketet utforskade alternativa tillvägagångssätt mot traditionell säkerhetstestning, e.x. ett publikt tillvägagångssätt för testning som kommer tillämpas på ett prototypsystem i vilka fordon och miljön interagerar med varandra.

Uppgift 4.3 Säkerhetsinformation (Ledare: VCC)

Tanken var att undersöka lösningar för säkerhetsdriftscenter och hur man samlar in, integrerar och behandlar data från olika källor tilll relevant handlingbar information för intressenter (IT-drift, myndigheter, serviceorganisationer samt forskning och utveckling). Under projektets gång gjordes dock en prioritering att

ytterligare resurser krävdes på Uppgift 3.4, intrångsdetektering/IDS, vilket resulterade i att *Uppgift 4.3 - Säkerhetsinformation*, inte exekverades under projektets tid.

Konkreta leveranser
Utöver nedanstående så har det också gjorts ett antal publiceringar inom området. Dessa är listade under *7.2 Publikationer.*

D4.1 Tailloring the HEAVENS risk assessment methodology for improved performance
D4.2 Secure Software Verification & Validation
D4.3 HoliSec Reference Architecture

Resultat
4.1. Det viktigaste bidraget till denna uppgift har varit skapandet av avancerade analysmetoder för identifiering av datasäkerhetshot. Den första tekniken (eSTRIDE) riktar sig mot att förbättra effektiviteten av hotmodellering genom att på ett snabbare sätt leda datasäkerhetsexperterna till identifiering av viktiga hot. Den andra tekniken (SecDFD), fokuserar på formella metoder och ger ett automatiserat verktyg för analysen av datasäkerhetsproblem i flödesorienterade, tillgångscentrerade modeller. Dessa tekniker har definierats som ett sätt att överkomma begräsningarna hos existerande tekniker.

4.2. Kombinationen av hög mobilitet och trådlös kommunikation i många säkerhetskritiska system har ökat deras exponering för skadliga säkerhetshot. Tidigare arbeten har föreslagit lösningar för att säkerställa funktions- och informationssäkerhet för dessa system. Mindre uppmärksamhet har givits till samspelet mellan dessa två grupper av icke-funktionella krav. Detta är ett problem då funktionssäkerhetslösningar kan påverka informationssäkerhetslösningar negativt och vice versa. Arbetet adresserar samspelet mellan funktionssäkerhet och informationssäkerhet genom att föreslå ett attackinjiceringsramverk, baserat på modell-implementerad felinjicering, lämplig för modell-baserad design. Ramverket gör det möjligt att studera och utvärdera effekterna av cybersäkerhets-attacker på systemsäkerhet tidigt i utvecklingsprocessen. För att uppnå detta har vi implementerat sex attackinjiceringsmodeller och genomfört experiment på Simulink-modeller av en CAN-buss och en brake-by-wire-styrenhet. Resultaten visar att de modellerade säkerhetsattackerna kan påverka systemsäkerheten negativt då de definierade säkerhetskraven ej uppfylldes.

En bug bounty fanns initialt i planen för HoliSec-projektet [1]. På grund av svårigheter med att samla alla resurser som behövdes för att genomföra aktiviteten under samma period så flyttades eventet två gånger för att slutligen ställas in. En stor del av förberedelserna hann genomföras innan dess. Resultatet av detta är BusGoat, en mock-up ECU som används som urvalsmekanism för bug-jägare. Denna har vidareutvecklats och använts nu i ett annat Vinnova-finansierat projekt för att genomföra utbildning inom cybersäkerhet för utvecklare och testare i fordonsindustrin.

Vidare har det genomförts en systematisk genomgång av existerande forskning relaterad till bug bounties och en intervjustudie som syftar till att undersöka upplevda fördelar, samt möjliggörare och barriärer för bugg-bounties inom fordonsindustrin. Arbetet har resulterat i tre vetenskapliga artiklar, varav en är accepterad för publikation, en är under review och den sista är planerad att lämnas in innan året (2019) är slut. Se *7 Spridning och Publicering*

4.3. Under projektets gång gjordes en prioritering att ytterligare resurser krävdes på Uppgift 3.4, intrångsdetektering/IDS, vilket resulterade i att *Uppgift 4.3 - Säkerhetsinformation*, inte exekverades under projektets tid.

6.6 [WP 5] Demonstration och Spridning

Beskrivning av innehåll
Arbetspaketet demonstrerade och spred resultat (koncept och metoder) från projektet .

Konkreta leveranser
Framtagning av utrustning för demonstration.

Resultat
Resultatet är en framgångsrik implementation av den nya SecOC modulen samt mätning av dess effektivitet. En fallstudie genomfördes på svarstiden vid nedtryckning av bromspedal samt när bromsljuset tänds med säker kommunikation mellan två ECU:er. Resultatet visar att denna autentiseringsmekanism är mycket effektiv. Vidare har också en metod för säker nyckelhantering och hantering av färskhet (”*Freshness Value”*) med framgång uppnåtts.

6.7 Måluppfyllelse

Projektet HoliSec[1] levererade de mål som sattes upp genom ett effektivt samarbete mellan partners (akademin, SMEer och OEM:er inom fordonsindustrin). Genom de olika arbetspaketen har säkerhetsteknologier undersökts, testats och anpassats till kontexten för fordonsindustrin **[Obj3]**. Inledningen av projektet [WP1] har levererat en uppdaterad State-of-the-Art och Needs/Requirements vilket säkerställt att processerna och teknologierna som undersökts ligger i linje med existerande datasäkerhetsstandarder **[Obj4]**. Det goda samarbetet med akademiska partners, SMEer och OEM:er inom fordonsindustrin har bidragit till utveckling av gemensamma processer/metoder/regelverk samt ökning av den svenska kapaciteten inom forskning och innovation vilket gynnat den svenska fordonsindustrin och akademin **[Obj2] [Obj5] [Obj6]**. Projektet har finansierat en industridoktorand och två licentiat-examina. Tillsammans bidrar resultaten av uppgifterna i projektet till att förstå utmaningar med datasäkerhet och associerade säkerhets-, integritets-, finansiella, och operationella risker**[Obj1]**.

De flesta av uppgifterna som var planerade från projektets start har framgångsrikt levererats med undantag för två avvikelser.

(1) Under projektets gång gjordes en prioritering att ytterligare resurser krävdes till Uppgift 3.4, intrångsdetektering/IDS, vilket resulterade i att *Uppgift 4.3 - Säkerhetsinformation*, inte exekverades under projektets tid.

(2) Att ordna ett bugbounty-event enligt Uppgift 3.4, visade sig till slut inte genomförbart då det blev problem att samla alla resurser. Efter tre försök så togs beslutet att inte genomföra eventet. En stor del av förberedelserna hann dock genomföras innan dess vilket resulterat i BusGoat, en mock-up ECU som används som urvalsmekanism för bug-jägare. Denna har vidareutvecklats och används nu i ett annat vinnovafinansierat projekt för att genomföra utbildning inom cybersäkerhet för utvecklare och testare i fordonsindustrin.

7 Spridning och publicering

7.1 Kunskaps- och resultatspridning

Hur har/planeras projektresultatet att användas och spridas?	Markera med X	Kommentar
Öka kunskapen inom området	X	Projektet har samlat data både från den akademiska världen och från domänexperter i industrin. Resultat och diskussioner har medfört kunskapsökning inom akademi och industri. Projektet har också resulterat i en doktorsexamen och två Teknologie Licentiat-examina samt ett flertal examensarbeten.
Föras vidare till andra avancerade tekniska utvecklingsprojekt	X	Resultatet har presenterats på flertalet konferenser i forskningsvärlden, samt utgör basen för det fortsatta samarbetsprojektet mellan akademiska partners samt företag inom fordonsindustrin.
Föras vidare till produktutvecklingsprojekt	X	Domänexperter hos respektive partner inom fordonsindustrin har involverats både i frågeställningar och resultat.
Introduceras på marknaden		
Användas i utredningar/regelverk/ tillståndsärenden/ politiska beslut		

7.2 Publikationer

"A Study of the Interplay Between Safety and Security Using Model-Implemented Fault Injection"
in Proc. 14th European Dependable Computing Conference (EDCC), Lasi, Romania, 2018.
Behrooz Sangchoolie. Peter Folkesson, Jonny Vinter

"*What the Stack? On Memory Exploitation and Protection in Resource Constrained Automotive Systems"*
Critical Information Infrastructures Security: 12th International Conference,
CRITIS 2017
Aljoscha Lautenbach, Magnus Almgren and Tomas Olovsson

"Secure software development for automotive systems – Implementation pitfalls in AUTOSAR"
Technical Report 2017:06, ISSN 1652-926X
Aljoscha Lautenbach, Magnus Almgren and Tomas Olovsson

"Open Problems when Mapping Automotive Security Levels to System Requirements"
Presented at 4th International Conference on Vehicle Technology and Intelligent Transport Systems, VEHITS 2018 (http://vehits.org) Funchal, Madeira, Portugal, 2018-03-16 - 2018-03-18
Thomas Rosenstatter and Tomas Olovsson

"Towards a Standardized Mapping from Automotive Security Levels to Security Mechanisms"
IEEE Conference on Intelligent Transportation Systems, Proceedings, ITSC, p.1501-1507
Thomas Rosenstatter and Tomas Olovsson

"Understanding common automotive security issues and their implications"
International Workshop on Interplay of Security, Safety and System/Software Architecture
Barcelona, , 2018-09-07 – 2019-09-07
Aljoscha Lautenbach, Magnus Almgren and Tomas Olovsson

“A risk assessment framework for automotive embedded systems”
CPSS ’16 Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security
M. Islam, A. Lautenbach, C. Sandberg, T. Olovsson
”In-vehicle CAN message authentication: An evaluation based on industrial criteria”
2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)
Nasser Nowdehi, Aljoscha Lautenbach, Tomas Olovsson

“*Securing the Connected Car”*
IEEE Vehicular Technology Magazine (1), p. 56-65
Kim Strandberg, Tomas Olovsson, Erland Jonsson

“M. Design and implementation of an intrusion detection system (IDS) for in-vehicle networks”
Master thesis at the department of Computer Science and Engineering (CSE), Chalmers University of Technology, 2017
Salman, N., & Bresch

“CAN-Aware Stealthy-Attack Detection for In-Vehicle Networks”
Submitted to the 2019 Annual Computer Security Applications Conference (ACSAC), 2019
Nowdehi, N., Aoudi, W., & Olovsson, O. Casad

”Lightweight Intrusion Detection System for In-Vehicle Communication on CAN”
Master thesis at the department of Computer Science and Engineering (CSE), Chalmers University of Technology, 2019
Kvarnström, S., Thiringer, D. A

“*Towards security threats that matter*”
Workshop on the Security of Industrial Control Systems & Of Cyber-Physical Systems (CyberICPS), 2017
Katja Tuma, Roccardo Scandariato, Mathias Widman, Christian Sandberg

“*Flaws in Flows: Unveiling Design Flaws via Information Flow Analysis*”
International Conference on Software Architecture (ICSA), 2019
Katja Tuma, Musard Balliu, Riccardo Scandariato

“*Privacy Compliance via Model Transformations*”
International Workshop on Privacy Engineering (IWPE), 2018
Thibaud Antignac, Riccardo Scandariato, Gerardo Schneider

“*Threat analysis of software systems: A systematic literature review*”
Journal of Systems and Software, Volume 144, Pages 275-294, 2018
Katja Tuma, Gul Calikli, Riccardo Scandariato

“*Two Architectural Threat Analysis Techniques Compared*”
European Conference on Software Architecture (ECSA), 2018
Katja Suma, Riccardo Scandariato

“Bug Bounty Programs - A Mapping Study”
Euromicro conference on Software Engineering and Advanced Applications, 2019
Ana Magazinius, Niklas Mellegård, Linda Olsson

"What we Know About Bug Bounty Programs - an Exploratory Systematic Mapping Study”
ESORICS 2019, European Symposium on Research in Computer Security
Ana Magazinius, Niklas Mellegård, Linda Olsson

“Automotive Bug Bounties - Opportunities, Enablers and Barriers”

Ana Magazinius, Niklas Mellegård

"Secure Data-Flow Compliance Checks between Models and Code based on Automated Mappings"
International Conference on Model Driven Engineering Languages and Systems (MODELS), 2019
Sven Peldszus, Katja Tuma, Daniel Strüber, Jan Jürjens, Riccardo Scandariato

"Towards Automated Security Design Flaw Detection"
International Workshop on Software Security from Design to Deployment (SEAD), 2019
Laurens Sion, Katja Tuma, Riccardo Scandariato, Koen Yskout, Wouter Joosen

"Inspection Guidelines to Identify Security Design Flaws"
International Workshop on Designing and Measuring CyberSecurity in Software Architecture (DeMeSSA), 2019
Katja Tuma, Daniel Hosseini, Kyriakos Malamas, Riccardo Scandariato

"Towards a Standardized Framework for Securing Connected Vehicles"
Thomas Rosenstatter
Licentiatavhandling

"On Securing Vehicular Communications: Methods and Recommendations for Secure In-vehicle and Car2X Communications"
Nasser Nowdehi
Licentiatavhandling

"Towards Efficiency and Quality Assurance in Threat Analysis of Software Systems"
Katja Tuma
Licentiatavhandling

7.3 DEx

Som ett resultat av HoliSec [1], och behovet av informationspridning associerad med projektet så har även ett bevaknings- och spridningsuppdrag, benämnt DEx, använts. Detta var ett initiativ för att bevaka och sprida information om forskningsprojekt via webben (https://autosec.se/) samt genomföra regelbundna konferenser och workshops.

Kunskap och information framtagen under projektet HoliSec [1] har därför utöver övriga publikationer också presenterats på www.autosec.se. Dessutom så har även resultat presenterats på nedanstående DEx-konferenser.

Katja Tuma - "*eSTRIDE: finding security threats that matter*" - FFI AutoSec Conference Fall, DEx 2018

Katja Tuma - "*Evolving Threat analysis Techniques to Catch What Matters*" - FFI AutoSec Conference Fall, DEx 2019

8 Slutsatser och fortsatt forskning

Projektet HoliSec [1] har fokuserat på att öka medvetenheten för hur potentiella datasäkerhetshot kan och skall bemötas med teknologier, samt vilka datasäkerhetskomponenter som behövs. Historiskt har det inte varit så stor vikt i att implementera datasäkerhetsmekanismer som skyddar mot angrepp på fordonets komponenter, men nu när fordonen blir allt mer uppkopplade, och också går mot att vara helt autonoma så ökar såklart behovet att också integrera mekanismer som inte bara skyddar mot intrång utan även detekterar att ett intrång har skett. Teknologier som intrångsdetektering (IDS), kryptering av data samt validering av data har länge existerat för internetbaserade teknologier. Projektet HoliSec [1] visade, och demonstrerade att dessa tekniker går att anpassa för fordonsindustrin och för de teknologier som används i fordonen.

Slutsatser från projektet är att det genom analysmetoder för identifiering av säkerhetshot på ett effektivt sätt går att leda säkerhetsexperter till identifiering av viktiga datasäkerhetshot. Slutsatser är också att intrångsdetektering (IDS) är en användbar teknologi, om än från ett kostnadsperspektiv endast på de mest kritiska domänerna i fordonet. IDS ger en möjlighet att identifiera intrång på fordonets interna infrastruktur. Utöver det påvisas och demonstreras också i HoliSec [1] att teknologier som kryptering, meddelandeintegritet, autentisering, för skydd av data i fordonets nätverk är implementerbara i fordonsindustrin. Resultat från HoliSec [1] visar på förslag på tekniker för att implementera autentisering/validering av hårdvara som kopplas in i fordonets nätverk och då med möjlighet att blockera ej godkända- eller genom lagkrav ej tillåtna enheter.

Fortsatt forskning

Även om ovan tekniker är implementerbara så krävs dock ytterligare forskning inom funktionalitet som kan ta hand om data rörande ett intrång, analysera data och även ta beslut eller införa en åtgärd baserat på allvarlighetsgrad och påverkan på fordonet. Ännu viktigare är dettta stöd i autonoma fordon, där fordonet inte kan lämna över kontrollen till en förare, och kanske inte vid tillfället är anslutet till det globala nätverket. Besluten behöver tas på ett sådant sätt att fordonets trafiksäkerhet ej påverkas.

I samband med lagkrav från UNECE som ställer krav på att, (i) fordonet skall vara resilient mot cyber-attacker, och (2) fordonet skall ha möjlighet att identifiera cyber-attacker och ta beslut därefter, så pågår det nu ett annat Vinnova-projekt vid namn CyReV (Cyber Resillience for Vehicles) [5] som kommer fortsätta forskningen inom området men med fokus på vad som identifierar ett intrång, implementering en maskininlärningsteknik för beteendebaserad intrångsdetektering samt insamling av data för analys efter att ett intrång har inträffat. Vidare kommer också undersökas samspelet mellan funktionssäkerhet och cybersäkerhet.

9 Deltagande partners och kontaktpersoner

Arc Core
Kontaktperson: Mathias Kremer

Assured
Kontaktperson: Jonas Magazinius

Chalmers
Kontaktperson: Tomas Olovsson

RISE Electronics (SP Technical Research Institute of Sweden)
Kontaktperson: Jonny Vinter

RISE Viktoria (Viktoria Swedish ICT)
Kontaktperson: Stefan Pettersson

Volvo Car Corporation
Kontaktperson: Ulf Edvardsson

Volvo Technology
Kontaktperson: Lars-Olof Berntsson

10 Referenser

[1] FFI project HoliSec https://www.ri.se/en/what-we-do/projects/holistic-approach-improve-data-security-vehicles, Accessed: 2018-12-05

[2] FFI project HEAVENS, https://www.sp.se/en/index/research/dependable_systems/heavens/Sidor/default.aspx, Accessed: 2018-12-05

[3] ISO/SAE CD 21434, Road Vehicles -- Cybersecurity engineering, https://www.iso.org/standard/70918.html, Accessed: 2018-12-10

[4] ISO 26262:2011 Road vehicles-functional safety, ISO, Standard, 2011.

[5] CyReV (phase 1), https://www.vinnova.se/en/p/cyrev-phase1---cyber-resilience-for-vehicles---cybersecurity-for-automotive-systems-in-a-changing-environment/

[6] E-Safety Vehicle Intrusion Protected Applications (EVITA), https://www.evita-project.org/, accessed: 2018-12-10.