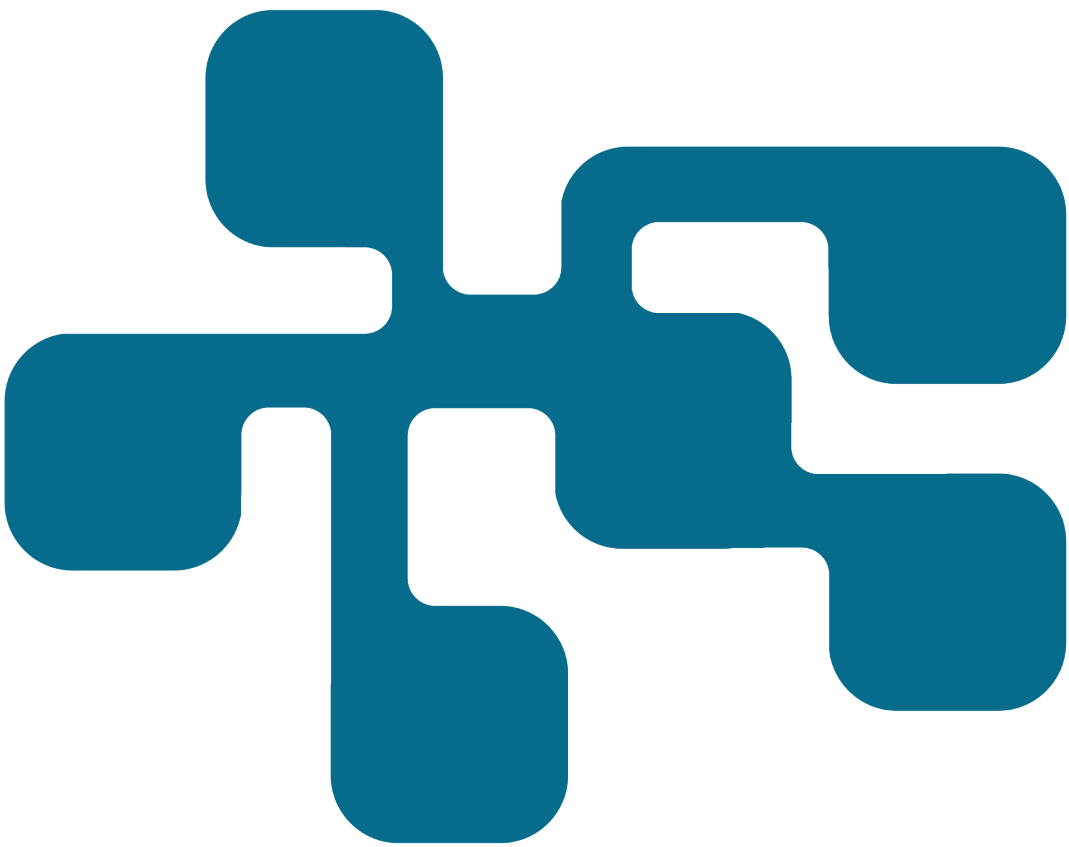
Cyberfysiska sårbarheter i tunga fordon

Med inriktning mot tunga fordon av vikt för civilförsvaret

CHRISTIAN VALASSI, MARTIN KARRESAND



FOI-R--5067--SE
ISSN 1650-1942 December 2020

Christian Valassi, Martin Karresand

Cyberfysiska sårbarheter i tunga fordon

Med inriktning mot tunga fordon av vikt för civilförsvaret

Titel	Cyberfysiska sårbarheter i tunga fordon– Med inriktning mot tunga fordon av vikt för civilförsvaret
Title	Cyber-physical Vulnerabilities in Heavy Vehicles
Rapportnr/Report no	FOI-R--5067--SE
Månad/Month	December
Utgivningsår/Year	2020
Antal sidor/Pages	56
ISSN	1650-1942
Kund/Customer	MSB
Forskningsområde	Informationssäkerhet
FoT-område	Inget FoT-område
Projektnr/Project no	E72567
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Ledningssystem

Sammanfattning

Fordon blir allt mer digitaliserade och förses med olika gränssnitt för uppkoppling mot internet och annan digital utrustning. Detta gäller inte minst tunga fordon, där olika påbyggnader från tredje part ytterligare ökar gränsytorna mot omvärlden. Samtidigt utgör en stor del av den tunga fordonsflottan en viktig del av samhällsviktig verksamhet. MSB har därför initierat en studie av cybersäkerhet i tunga fordon, med särskild inriktning mot fordon av vikt för civilförsvaret, för att belysa aktuell status och framtida trender inom området.

Studien har bedrivits inom NCS3-samarbetet och bygger på en litteraturstudie inom området samt intervjuer med personal på olika befattningar inom räddningstjänsten och fordonstillverkare. Resultatet visar att cybersäkerhets-arbetet inom branschen ännu är i sin linda, men att tillverkningssidan har börjat anamma cybersäkerhetsprinciper vid nyutveckling. Trots att cybersäkerhetsnivån i tunga fordon är låg samtidigt som angreppsytorna ökar motverkar delvis det traditionella fokuset på tillförlitlighet och personsäkerhet (eng. *safety*) risken för framgångsrika angrepp. Vår bedömning är att för närvarande utgör något slags tillgänglighetsangrepp det största hotet.

Nyckelord: cybersäkerhet, tunga fordon, industriella informations- och styrsystem

Summary

Vehicles are currently getting more and more digitalized and the number of interfaces exposed to the internet and other digital equipment are increasing. This is especially true for heavy vehicles, where different third party add-ons adds to the interfaces connecting to the rest of the world. At the same time a large part of the heavy vehicle fleet performs vital societal functions. MSB therefore has initiated a study of cyber security in heavy vehicles, focused on vehicles used in the civil defence operation of Sweden, to illuminate the current status and future trends within the area.

The study is part of the NCS3 collaboration and is conducted as a literature survey within the area, together with interviews with personnel having different roles within the civil protection services and vehicle manufacturing. The result shows that the cyber security work still is in its infancy, but that the manufacturing parties have started to adopt cyber security principles when developing new vehicles. In spite of the fact that the cyber security level is low at the same time as the attack surfaces are increasing the traditional focus on reliability and safety partially decreases the risk of successful attacks. Currently we estimate some sort of Denial-of-Service attack to pose the biggest threat.

Keywords: cyber security, heavy vehicles, industrial control systems

Innehållsförteckning

1 Inledning

Fordon, som mycket annat i dagens samhälle, ges allt större möjlighet för extern kommunikation och anslutning mot publika nätverk. Fordon är inte heller längre endast att anse som en samling mekaniska enheter utan styrs numera till stor del av elektroniska komponenter och datorer. Det har i ett flertal tidigare studier påvisats att cybersäkerhetsangrepp[1] mot fordon kan få svåra konsekvenser eftersom de kan påverka fordon under färd, vilket i sin tur kan få betydande konsekvenser för fordonets förare och passagerare samt för fordonets omgivning (Kennedy, Holt & Cheng 2019). Sammantaget innebär detta att cybersäkerhet bör ges en allt större roll i utvecklingen och tillverkningen av fordon.

Tidigare forskning, såväl som en majoritet av den forskning på området som utförs idag, fokuserar på cybersäkerhet relaterat till personfordon. Forskning om cybersäkerhet i tunga fordon har inte rönt lika stort intresse. Samtidigt finns det generellt inga eller mycket få exempel på verkliga cyberangrepp mot fordon.[2] Det är oklart vad detta beror på men Kennedy, Holt och Cheng (2019) spekulerar i att svaret delvis kan involvera den höga kunskapsmässiga tröskel som måste överstigas för att framgångsrikt påverka fordon via cyberangrepp.

Likväl kan konsekvenserna av framgångsrika angrepp mot fordon, oavsett vikt, vara betydande. Personsäkerheten kan äventyras, för såväl förare och passagerare som omgivning. För tunga fordon specifikt kan även bredare samhällspåverkan ses, exempelvis i form av transportbortfall för livsmedel, läkemedel eller andra varor eller tjänster av samhällsviktig natur. År 2019 transporterades exempelvis närmare 449 miljoner ton gods med svenska lastbilar inrikes, cirka 20 % av vilka utgjordes av livsmedelstransport (inkluderat råvaror från jordbruk, skogsbruk och fiske) (Trafikanalys 2019a). Jämförelsevis transporterades cirka 74 miljoner ton gods på järnväg samma år (Trafikanalys 2019b). Vidare kan samhällsviktiga tjänster i form av exempelvis räddningstjänst påverkas starkt av framgångsrika cyberangrepp mot tunga fordon.

1.1 Mål och Syfte

Totalförsvarets forskningsinstitut (FOI) har fått i uppdrag av *Myndigheten för samhällsskydd och beredskap* (MSB) att undersöka sårbarheter hos tunga fordon av betydelse för civilförsvaret.

Studien ska besvara följande frågeställningar:

[1] Notera att begreppet *angrepp* i rapporten kan likställas med cyberangrepp, om inget annat anges.

[2] Inom ramen för denna studie har inga verkliga angrepp hittats, vilket även beskrivs av Stachowski, Bielawski och Weimerskirch (2018).

- Vilken kommunikationskanal medför den största risken för att ett fordon otillbörligen kan påverkas (vid direkt fysisk kontakt, närhet eller på avstånd)?
- Vilka cybersäkerhetsrisker innebär tredjepartssystem/ombyggnationer av fordon?
    - Vilka konsekvenser kan dessa risker få?
- Hur utvärderar beställare sina specialleverantörer ur en cybersäkerhetssynvinkel?
- Vilken kunskap har berörda intressenter gällande cybersäkerhet i tunga fordon?

FOI genomförde 2017 en studie om tunga fordon (Gustafsson & Valassi 2018). Syftet med den studien var att översiktligt kartlägga system och teknologier som används i tunga fordon. Den här studien bygger vidare på det tidigare arbetet från 2017 genom att undersöka vilka sårbarheter som etablerade teknologier och system i tunga fordon kan medföra.

1.2 Metod

Innehållet i den här studien baseras primärt på information insamlad på två olika sätt. Information kopplad till allmänna koncept och teknik för tunga fordon samlades in genom en litteraturstudie. Information relaterad till resultat och slutsatser hämtades främst från de intervjuer som genomfördes under studien.

I inledningen av denna rapport beskrivs hur huvuddelen av forskningen inom cybersäkerhet i fordon fokuserar på personfordon och att forskningen kring cybersäkerhet i tunga fordon (ännu) inte rönt samma intresse. Det är oklart vad detta beror på, särskilt eftersom det finns indikationer på att cybersäkerhets-sårbarheter och -svagheter som existerar i personfordon även återfinns i tunga fordon. Exempelvis rapporterar den amerikanska motorvägs- och trafiksäkerhets-administrationen, *National Highway Traffic Safety Administration* (NHTSA) att många av de sårbarhetsfaktorer som dokumenterats för personfordon även återfinns i tunga fordon (Stachowski, Bielawski & Weimerskirch 2018). Detta innebär i sin tur att den forskning som utförs på personfordon även har viss bäring på tunga fordon. Därför har även tidigare personfordonsstudier inkluderats i underlaget till denna studie.

De intervjuer som genomförts i studien var av semistrukturerad karaktär, där frågorna baserats på studiens fyra huvudfrågeställningar. Dessa kompletterades även av frågor som uppdagats under den tidigare genomförda litteraturstudien. Intervjufrågorna återfinns i sin helhet i Bilaga A: Intervjuguide. Den semi-strukturerade karaktären av intervjuerna lämpade sig väl för denna studie eftersom den gav möjligheter till att ställa följdfrågor eller andra frågor som

uppdagades under själva intervjuerna. Vidare gavs även intervjurespondenter möjligheter att utveckla och resonera kring sina svar.

Urvalet av intervjurespondenter baserades till största del på ett icke-sannolikhets-baserat bekvämlighetsurval, vilket innebar att det inte fanns någon medveten slumpmässighet i urvalet av respondenter (Denscombe 2014). Respondenter för studiens intervjuer valdes ut baserat på organisation och arbetsroll, men även tillgänglighet, vilket representerar bekvämlighetsdelen av urvalet.

Majoriteten av respondenterna är verksamma inom räddningstjänsterna i olika delar av landet. Denna verksamhet har i studien bedömts som synnerligen intressant utifrån studiens syfte och mål med inriktningen på tunga fordon av betydelse för civilförsvaret. Det hade även varit relevant och intressant att inkludera andra verksamhetsområden för tunga fordon, vilka kan anses ha betydelse för civilförsvaret. Detta har dock inom ramen för studien inte varit möjligt, till största del på grund av tidsbrist.

Alla respondenter kontaktades via mejl vilka specificerade studiens uppdrag och omfång samt ställde frågan om respondenten vill ställa upp på en intervju. Efterföljande mejlkorrespondens inkluderade framförallt överenskommelse av tid, plats och metod för intervjugenomförandet eller förtydliganden kring studien, genomförandet eller intervjuerna. Det förfrågningsmejl som användes för den initiala kontakten med potentiella respondenter återfinns i Bilaga B: Intervjuförfrågan

Totalt genomfördes fem intervjuer med lika många individer från fyra olika organisationer.

1.3 Definitioner och avgränsningar

I svensk lag definieras ett tungt fordon som ett fordon med en totalvikt på över 3,5 ton. Definitionen delas i lagtext upp efter fordonstyp, vilket exempelvis innebär att ett tungt fordon av typen lastbil benämns som tung lastbil och ett tungt fordon av typen buss definieras som tung buss (SFS 2001:559). Utöver dessa definitioner finns även definitioner av lätt lastbil, lätt buss och lätt släpfordon vars totalvikt maximalt får uppstiga till 3,5 ton.

En personbil definieras enligt svensk lag som en bil som är

> *försedd med högst 8 sittplatser utöver förarplatsen och: (1) är inrättad huvudsakligen för personbefordran eller (2) är permanent försedd med ett karosseri som är inrättat som bostadsutrymme och utrustat med åtminstone (a) fast monterade sittplatser, (b) fast monterade sovplatser som kan utgöras av sittplatser som kan omvandlas till sovplatser, (c) fast monterad utrustning för matlagning och lagring och (d) bord. Personbilar delas in i två klasser klass*

> *I och klass II. Personbilar av klass I definieras som: Personbilar som inte tillhör klass II. Klass II definieras som en personbil som är permanent försedd med karosseri som är inrättat som bostadsutrymme och utrustat med (a), (b), (c) och (d) ovan* (SFS 2001:559).

Oftast registreras klass II personbilar som husbilar, men tyngre husbilar (över 3,5 ton) kan även registreras som lastbilar (Transportstyrelsen 2015).

Denna rapport behandlar endast tunga fordon och tar därför inte direkt hänsyn till fordon av typerna:

- Personbilar klass I
- Lätt lastbil
- Lätt buss
- Lätt släpfordon

Eftersom det finns ett visst överlapp mellan personbilar och tunga fordon vad gäller cybersäkerhetsproblematik (se avsnitt 1.2), är det även relevant att inkludera aspekter från personbilar när cybersäkerhet i tunga fordon diskuteras. Därför exkluderas inte lätta typer av fordon i rapporten, men fokus för studien är tunga fordon.

Angående den fysiska attackytan görs i denna studie en distinktion mellan direkt och indirekt fysisk tillgång. I detta avseende innebär indirekt fysisk tillgång att angriparen har möjlighet att angripa eller infektera enheter eller system vilka via fysiskt gränssnitt (kabel) ansluts till fordonets interna system av någon annan än angriparen själv. Studien ämnar endast inkludera angrepp eller sårbarheter vilka existerar och är möjliga att genomföra via indirekt fysisk tillgång. För vidare diskussion och resonemang kring detta se kapitel 4.

1.4 Läsanvisning

I det första kapitlet av denna rapport beskrivs en inledande problematik, rapportens mål och syfte introduceras. Därefter beskrivs datainsamlingsmetoder, samt vilka avgränsningar som gjorts för studien.

Kapitel 2 beskriver övergripande den interna kommunikationsarkitekturen för tunga fordon och vilka nätverksprotokoll som är vanligast förekommande. Där beskrivs även tredjepartssystem och hur dessa används inom tunga fordon. Kapitlet avslutas med en beskrivande diskussion kring skillnader mellan person-fordon och tunga fordon, utöver skillnader i intern kommunikationsarkitektur.

I kapitel 3 diskuteras tidigare forskning som utförts inom området och ett antal tidigare studier beskrivs tillsammans med deras resultat på en övergripande nivå.

Rapportens 4:e kapitel behandlar potentiella attackytor för tunga fordon och ger exempel på hur olika inbyggda enheter, komponenter och system i fordon kan utnyttjas av en potentiell antagonist.

I kapitel 5 diskuteras hur säkerhet hanteras i fordon, hur personsäkerhet kan påverka cybersäkerhet samt ges exempel på traditionella IT-säkerhetsmetoder som nyttjas inom fordon.

Kapitel 6 presenterar resultatet från de intervjuer som genomförts i studien.

I kapitel 7 diskuteras studiens resultat utifrån de genomförda intervjuerna och litteraturstudien.

Rapportens åttonde och avslutande kapitel presenterar de slutsatser som studien resulterat i.

Rapportens två bilagor innehåller intervjuernas frågeställningar samt den förfrågan som via mejl skickades till potentiella respondenter.

2 Bakgrund

Avsnitt i detta kapitel ger en övergripande beskrivning av tunga fordons kommunikationsarkitektur, tredjepartssystem samt skillnader och likheter mellan tunga fordon och personfordon.

2.1 Intern kommunikationsarkitektur och protokoll

Det finns skillnader och likheter mellan de interna kommunikationsarkitekturerna för personfordon och tunga fordon. Den primära skillnaden är att tunga fordon nyttjar standarden SAE J1939 för att definiera de interna kommunikations-bussarna[3] medan personfordon och andra lättare fordon ofta implementerar olika proprietära versioner av protokollet *Controller Area Network* (CAN). Andra kommunikationsbussar för icke-kritiska och kringliggande system har stora likheter mellan fordonstyper. Avsnitten 2.1.1 – 2.1.3 beskriver CAN, SAE J1939 samt andra relevanta kringliggande protokoll. Dessa beskrivningar är dock inte uttömmande utan fokuserar på att introducera respektive protokoll och illustrera skillnader samt likheter mellan dem.

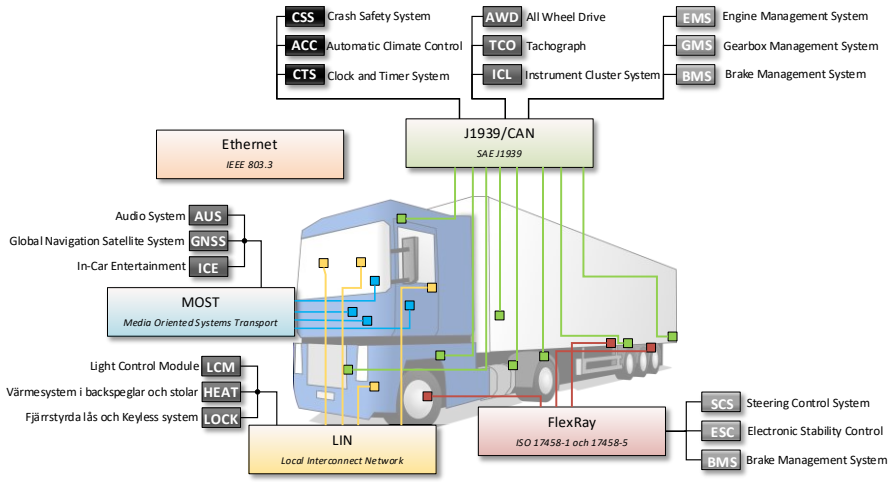
Inom alla typer av fordon används styrenheter, vilka inom fordonsindustrin generellt benämns *Electronic Control Unit* (ECU). Dessa styrenheter har likheter med industriella styrenheter inom andra branscher eftersom det i huvudsak rör sig om robusta beräkningsenheter med specifika uppgifter, men som i hög grad nyttjar branschspecifika standarder och kommunikationsprotokoll. De operativ-system som används för denna typ av enheter är generellt mycket enkla och inte designade för att hantera specialskriven kod. Däremot är operativsystemen ofta designade för att vara driftsäkra, dock inte ur ett cybersäkerhetsperspektiv (Stachowski, Bielawski & Weimerskirch 2018).

Det är vanligt att styrenheterna ges namn baserat på det system de ingår i, till exempel *Brake Control Module* (BCM) och *Transmission Control Unit* (TCU). Namn, förkortningar och systemens funktion skiljer sig ofta mellan tillverkare och det förekommer också att en förkortning återanvänds men med annan betydelse. Det är därför viktigt att kontrollera innebörden av en term för att kunna jämföra system mellan olika tillverkare.

[3] En kommunikationsbuss är ett system av gemensamma ledningar som förbinder digitala moduler och som används inom fordonsindustrin för att beskriva nätverket mellan olika enheter. Inom fordonsindustrin används ofta singularformen även om moderna fordon i regel innehar flera kommunikationsbussar som ofta är segmenterade och som ibland använder olika nätverksprotokoll.

Antalet styrenheter som finns i fordon varierar baserat på tillverkare, tillverkningsår, modell och fordonets funktioner. Dagens fordon innehåller vanligtvis cirka 100 stycken ECU:er och lyxmodeller för personfordon uppemot 150 stycken ECU:er, som alla ansluts till, och kommunicerar över, en eller flera kommunikationsbussar i fordonet (Winning 2019). Vidare innehåller moderna fordon uppemot 100 miljoner rader programkod (Informationisbeautiful 2015). Sammantaget innebär detta att fordon utöver dess mekaniska funktioner även är mycket komplicerade rent IT-mässigt.

I figur 1 visas ett exempel på nätverksprotokoll och hur de kan användas i moderna tunga fordon.



Figur 1. Nätverksprotokoll i ett modernt tungt fordon och ett exempel på hur dessa protokoll kan användas. Observera att användningen varierar med tillverkare, modell och tillverkningsår (Gustafsson och Valassi 2018).

2.1.1 Controller Area Network (CAN)

Controller Area Network (CAN) är ett multi-master seriellt bussprotokoll som definieras av standardsamlingen ISO 11898. CAN möjliggör tillförlitlig överföring av datapaket i ett fysiskt medium bestående av två sammanflätade kopparkablar. Protokollet tillåter en överföringshastighet på upp till 1 Mbit/s[4] (cirka 8 Mbit/s för CAN Flexible Data-Rate) och kan effektivt hantera fel och återhämtning. CAN utgör kommunikationsgrunden för majoriteten av alla fordon oavsett typ (Mukherjee, Van Etten, Samyukta, Walker, Ray & Ray 2019).

[4] Det bör noteras att överföringskapacitet för CAN är direkt beroende av kabellängd. CAN-nätverk har exempelvis en teoretisk maximal kabellängd på 6000 meter med en överföringshastighet på upp till 1 kbit/s

CAN bygger på *Open Systems Interconnect*-modellen (OSI) och omfattar lager 1 (fysiskt skikt) samt 2 (datalänkskikt). Funktioner ur övriga lager (3-7) implementeras ofta inte explicit. Däremot inkluderar applikationsskiktet i vissa implementationer även funktionalitet från transportskiktet. Själva CAN-protokollet specificerar bara hur datapaket ska transporteras från punkt A till punkt B med hjälp av ett delat kommunikationsmedium. Protokollet saknar specifikation för hur kommunikation, flödeskontroll, transport av större data-paket eller adresshantering ska etableras. För att hantera sådan funktionalitet i kommunikationen måste dessa aspekter definieras av systemdesignern eller genom implementationen av ett protokoll i ett högre lager (eng. *Higher layer protocol* (HLP)). Det finns många HLP för CAN, några exempel är J1939, CANopen, MilCAN och Modbus (ISO 11898-1:2015; Johansson, Törngren & Nielsen 2005; Richards 2002).

CAN är ett meddelandebaserat protokoll och är alltså inte adressbaserat vilket innebär att enheter inte kommunicerar direkt med varandra. Istället sker kommunikation av datapaket i CAN genom att enheter bredsänder (eng. *broadcast*) paket, vilket innebär att alla enheter kan höra all kommunikation i nätverket. Det går alltså inte att bara skicka datapaket till en specifik enhet i nätverket. Hårdvaran i dessa nätverk filtrerar dock bort den kommunikation som inte är ämnad för enheten i fråga (Stachowski, Bielawski & Weimerskirch 2018; Pazul 1999).

För att upptäcka och hantera kommunikationskollisioner, exempelvis att två enheter sänder paket samtidigt, används ett *Media Access Controll*-protokoll (MAC). Specifikt är det *Carrier Sense Multiple Access/Collision Detection + Bitwise Arbitration*[5] (CSMA/CD+BA) vilket är en variant av det MAC-protokoll som tidigare användes för Ethernet. Protokollet kan något förenklat beskrivas som att, vid händelse av kollision, det vill säga att två enheter försöker skicka paket samtidigt kommer kommunikationen med högst prioritet att skickas. Den enhet som skickade den lägre prioriterade kommunikationen väntar en förut-bestämd tid innan nästa försök görs (Stachowski, Bielawski & Weimerskirch 2018; Richards 2002; Pazul 1999).

Nästa avsnitt beskriver standardsamlingen J1939 vilken nyttjas för kommunika-tionsbussen i majoriteten av tunga fordon. Det ska dock understrykas att tunga fordon även använder CAN i olika utsträckning, exempelvis kan proprietära CAN-versioner användas i segmenterade delsystem i ett tungt fordon. Utöver detta bygger även J1939 på CAN-protokollet, vilket innebär att CAN inte bara är viktigt att diskutera i relation till personfordon utan även för tunga fordon.

[5] Bitwise Arbitration (BA) benämns även som AMP eller CR, för *Arbitration on Message Priority* respective *Collision Resistance*.

2.1.2 SAE J1939

J1939 är en öppen standardsamling som utvecklats av SAE International och används i den interna kommunikationsbussen för en majoritet av tunga fordon världen över. J1939 är baserat på CAN och inkluderar utöver specifikationerna i CAN även standarder för hur datapaket bland annat ska sättas samman och tolkas. J1939 är ett HLP som använder CAN som underliggande lager (fysiskt skikt och datalänkskikt) enligt OSI-modellen (Mukherjee et al. 2019).

En standardiserad struktur för sammansättning och tolkning av datapaket innebär att olika tillverkare av tunga fordon och komponenter för dessa kan använda samma kommunikationsstandard. Detta medför exempelvis en förenklad konstruktionsprocess eftersom delkomponenter inte behöver specialiseras efter tillverkare av tunga fordon. Vidare innebär standardiseringen förenklad informationsinsamling och informationsutbyte inom och mellan olika typer av fordonsflottor.

2.1.3 Andra vanliga kommunikationsprotokoll

Det finns ett antal protokoll utöver CAN och J1939 som används inom tunga fordon. Dessa hanterar dock ofta icke-kritiska och kringliggande system (undantaget FlexRay) som media eller klimat- och komfortsystem. De vanligast förekommande av dessa protokoll är *Local Interconnect Network* (LIN) och *Multimedia Oriented Systems Transport* (MOST). Utöver dessa protokoll beskriver detta avsnitt även *FlexRay*, vilket är ett bussprotokoll likt CAN som används för kritiska delsystem inom fordon. Det är oklart om FlexRay i framtiden helt kan ersätta CAN-standarden men om så är fallet får detta även implikationer för tunga fordon, och därför beskrivs protokollet i detta avsnitt.

***Local Interconnect Network* (LIN)** är ett seriellt nätverksprotokoll med relativt låg dataöverföringskapacitet (20–40 kb/s). Protokollet är framtaget som ett billigare alternativ till CAN, att använda för system i fordon med lägre krav på robusthet och prestanda. LIN används därför i icke-kritiska delsystem som inte kräver överföring av större mängder data. Exempelvis används LIN för elektroniskt styrda backspeglar, säten och klimatsystem samt diverse funktionsknappar på ratten.

LIN implementeras som ett *källa-kopia*-protokoll vilket innebär att protokollet inte kräver vidare implementation av kollisionshanteringsfunktioner eftersom all kommunikation initieras av *käll*-noden.

Sedan LIN-konsortiets upplösning år 2010 hanteras LIN-standarden numera av *International Standards Organization* (ISO). Den senaste versionen av standarden publicerades i åtta delar år 2016 (ISO 17987-1-8:2016).

***Multimedia Oriented Systems Transport* (MOST)** är ett multimediaprotokoll som används för video, ljud och liknande datasignaler i fordon. Protokollet har

en relativt hög överföringshastighet (150 Mbit/s) i jämförelse med andra protokoll som används inom fordon. Protokollet lämpar sig väl för hantering av media dels på grund av dess hastighet men även på grund av dess anpassningsbarhet och *plug-and-play*-integration. Således är MOST ett väl lämpat komplement till CAN i de delar av kommunikationsbussen som behöver hantera tyngre nätverkstrafik och används därför i mycket stor utsträckning inom fordonsindustrin.

MOST använder *Time Division Multiplexing* (TDM) och CSMA för kollisionshantering av kommunikation. TDM växlar cykliskt och synkroniserat mellan olika datasignaler över en gemensam kommunikationslina. Varje kommunicerande enhet i nätverket har en specifik tidsram under vilken enhetens kommunikation överförs. Därefter får enheten vänta på sin nästa allokerade tidsram innan ytterligare kommunikation kan ske. Metoden går således ut på att undvika kollisioner, än att hantera dem.

FlexRay är ett protokoll grundat av Flexray-konsortiet i början av 2000-talet. I konsortiet ingår bland annat större fordonstillverkare såsom BMW AG, Volkswagen AG, Daimler AG och General Motors. Första implementationen av FlexRay i ett kommersiellt fordon skedde år 2006 i en BMW X5, men protokollet implementerades först fullt ut år 2008 i BMW 7-modellserien (Strobel 2013).

Protokollet har en överföringshastighet på 10 Mbit/s och använder till skillnad från CAN och J1939 *Time Division Multiple Access* (TDMA) för kollisionshantering av kommunikation. TDMA kontrollerar kommunikation mellan enheter med en gemensam tidssynkronisering vilket minskar sannolikheten för kollisioner.

FlexRay är designat för att vara snabbare och mer pålitligt än CAN, men är som en konsekvens samtidigt mer kostsamt. Det är oklart om FlexRay i framtiden helt kommer att ersätta CAN. Denna oklarhet kan delvis ha sin förklaring i att FlexRay i jämförelse med CAN är relativt nytt och oprövat samt att det är mer kostsamt. I dagsläget används FlexRay endast som ett komplement i säkerhetskritiska delsystem av fordon som kräver realtidskommunikation och redundans.

2.2 Tredjepartssystem

Tredjepartssystem definieras i denna rapport som system installerade i fordon av en leverantör som inte är originaltillverkaren, ofta kallad *Original Equipment Manufacturer* (OEM).

Tredjepartssystem kan användas för olika ändamål, men för tunga fordon är den vanligast förekommande typen av tredjepartssystem olika former av fordonsparksförvaltningssystem (eng. *Fleet Management System* (FMS)). FMS är

telematiksystem som nyttjas för att centralt övervaka fordons hälsa, utföra diagnostik och överföra logistiska data så som position och rutt.

I många fall ansluts FMS-lösningar direkt till den interna kommunikationsbussen ofta direkt via kommunikationsbussens fysiska kablage. Detta riskerar att påverka fordonets elektroniska styrsystem på ett sätt som varken tredjepartsleverantören, tillverkaren eller ägaren avsett eller insett (Stachowski, Bielawski & Weimerskirch 2018). Europeiska fordonstillverkare, däribland Volvo och Scania, tillåter inte denna typ av anslutning direkt på den interna kommunikationsbussen och har i ett brev till EU beskrivit att sådana anslutningar som extremt farliga och att dessa anslutningar förverkar fordonets garanti (FMS-standard 2004). Dessa anslutningar använder även i regel någon form av kommunikationslänk för extern kommunikation som dessutom ofta är permanent så länge fordonet har mobildatatäckning, vilket kan utgöra en möjlig vektor för cyberangrepp mot fordonet. Det blir dock allt vanligare att fordonstillverkare utvecklar och implementerar sina egna FMS i fordonen de tillverkar. Det har dock visat sig att kunder fortfarande installerar FMS från tredje part i sina fordon i syfte att bibehålla homogenitet i fordonsflottan (Stachowski, Bielawski & Weimerskirch 2018).

Stachowski, Bielawski och Weimerskirch (2018) menar att ett relaterat orosmoment till FMS är att om en sårbarhet upptäcks i ett FMS och en antagonist sedan finner en sårbarhet i ett fordon som nyttjar detta FMS kan detta få stora konsekvenser för hela fordonsflottan. Detta eftersom att fordonsflottor tenderar att vara homogena, vilket innebär att sårbarheterna kan utnyttjas i en majoritet av flottans fordon.

Vidare erbjuder flera brukare av tunga fordon möjligheter att spåra fordon, vilket bland annat kan användas internt eller av kunder för att exempelvis spåra leveranser av gods eller var i sin rutt en buss befinner sig. Stachowski, Bielawski och Weimerskirch (2018) menar att möjlighet till att spåra fordon kan leda till integritetsrelaterade problem. Avslöjande av exempelvis data rörande innehållet i ett lastat fordon tillsammans med möjligheten att spåra fordonet kan bidra till ökade stölder, antingen direkt från fordonet eller när godset har levererats till kund.

2.2.1 Påbyggnadsgränssnitt

Många tillverkare av tunga fordon implementerar så kallade påbyggnadsgränssnitt (eng. *body builder interface*) i syfte att förenkla påbyggnader för tredjepartsleverantörer. Många påbyggnationer behöver anslutning till fordonets interna kommunikationsbuss varför sådana anslutningar förbereds av tillverkaren. Hur dessa anslutningar förbereds skiljer sig mellan tillverkare och även mellan typer av tänkta påbyggnationer. En del tillverkare har standardkonfigurationer för en rad olika typer av påbyggnationer, exempelvis för brandbilar, bärgningsbilar, mobilkranbilar eller sopbilar. Sådana typer av

standardmallar har olika behov av anslutning till fordonets interna kommunikationsbuss.

Originaltillverkare av tunga fordon så som Scania och Volvo ställer specifika krav på alla former av ombyggnads- eller påbyggnadsarbeten på tunga fordon som de producerar. Dessa krav specificeras vanligen i form av ett antal anvisningar som måste följas av påbyggnadsleverantörer. Utöver anvisningarna måste även alla påbyggnader godkännas av en behörig representant från original-tillverkaren och följa rådande lagstiftning. Om anvisningar inte följs och godkännande inte söks av leverantören gäller inte fabriksgarantin för fordonet.

Scania (2017) beskriver i sina anvisningar att leverantörer som önskar utföra påbyggnationer som inte beskrivs i anvisningarna måste ansöka om godkännande av en behörig representant på Scania som i sin tur söker godkännande internt. Vidare beskriver anvisningarna att Scania endast kan tillhandahålla information och rekommendationer baserat på kända förutsättningar och att påbyggnadsleverantören ansvarar för:

- Att chassikomponenterna behåller sin ursprungliga funktion och kvalitet efter påbyggnadsarbetet
- Att påbyggnadsarbetet uppfyller juridiska, säkerhetsmässiga och hållbarhetsrelaterade krav
- Egenskaperna för hela fordonet i den utsträckning dessa påverkas av påbyggnaden.

Slutligen påpekas att både Scaniaåterförsäljaren och påbyggaren ansvarar för att se till att nödvändiga instruktioner och information medföljer fordonet vid leverans till kund (Scania 2017).

2.3 Personfordon och tunga fordon, skillnader och likheter

Det finns, utöver skillnader i den interna kommunikationsarkitekturen mellan tunga fordon och personfordon, även andra skillnader och likheter. I det här avsnittet diskuteras relevanta skillnader och likheter mellan tunga fordon och personfordon på en översiktlig nivå. I vissa fall finns det skillnader eller likheter som lämpar sig bättre i andra delar av rapporten. Dessa tas då upp där istället.

För tunga fordon är tillverkningsår en relevant aspekt att beakta i förhållande till cybersäkerhet. Detta beror på att många tunga fordon, oavsett tillverkare, typiskt nyttjar samma delkomponenter från samma leverantörer (Wiemerskirch, Becker & Hass 2017; Jonson 2018; Tollefson 2019). I förlängningen innebär homo-geniteten i komponentanvändandet att en sårbarhet i en specifik modell också troligtvis återfinns i andra modeller av samma modellår från andra tillverkare. Sammantaget betyder detta att en cybersäkerhetsmässig sårbarhet i ett tungt

fordon potentiellt kan få mycket stor spridning och påverkan i jämförelse med en liknande sårbarhet för personfordon. För personfordon kan samma homogenitet existera i de komponenter som används för flera modeller från samma tillverkare, men troligtvis inte mellan olika tillverkare (Stachowski, Bielawski & Weimerskirch 2018).

Vidare implementerar oftast personfordonstillverkare proprietära versioner av CAN för den interna kommunikationsarkitekturen i de fordon som tillverkaren producerar. J1939 som primärt nyttjas inom tunga fordon är å andra sidan en öppen standard vilket också innebär att den är mer åtkomlig för potentiella antagonister. Tunga fordon använder också proprietära versioner av CAN, dock gäller detta oftast endast för isolerade delsystem. Som med homogeniteten av komponenter påverkar även användandet av proprietära versioner av CAN spridningen och de möjliga konsekvenserna av en sårbarhet. Det är exempelvis svårare för en potentiell angripare att rekonstruera (eng. *reverse engineer*) en specifik proprietär CAN-version. För personfordon får alltså en sårbarhet i en proprietär version av CAN troligtvis mindre spridning än en liknande sårbarhet i J1939.

Den interna kommunikationsarkitekturen i personfordon implementeras ofta med en central nätsluss (eng. *gateway*) för att förenkla segmentering av interna kommunikationsbussar. Tunga fordon tenderar att implementera plattare arkitekturer utan centrala nätslussar för segmentering (Stachowski, Bielawski & Weimerskirch 2018).

Många skillnader mellan personfordon och tunga fordon återfinns, inte helt oväntat, i de fysiska aspekterna av fordonstyperna. Två exempel på sådana skillnader gäller styrnings- och bromssystem. För personfordon finns flera vanliga typer av styrningssystem, vilka är vakuumassisterade hydrauliska servosystem, elektrohydrauliska servosystem och helt elektriska servosystem. För tunga fordon nyttjas vanligen fortfarande hydrauliska servosystem, dock har vissa tillverkare påbörjat en övergång till den nyare generationen av elektriska servosystem.

För bromssystem i personfordon används i regel skivbromssystem där många system även inkluderar avancerade funktioner så som elektronisk stabilitets-kontroll (eng. *Electronic Stability Programme* (ESP)), antispinn (eng. *Traction Control System* (TCS)), rullningskontroll (eng. *Roll Stability Control* (RSC)), låsningsfria bromsar (ty. *Antiblockiersystem* (ABS)) och automatisk nödbroms (eng. *Emergency Brake Assist* (EBA)). Tunga fordon implementerar vanligen pneumatiska bromssystem, men inkluderar även många av de funktioner som återfinns i personfordon som exempelvis ABS, ESP, EBA och RSC. I Europa blir det allt vanligare att dessa pneumatiska system hanteras elektroniskt (Stachowski, Bielawski & Weimerskirch 2018).

En annan tydlig skillnad mellan personfordon och tunga fordon gäller motiverande faktorer för införskaffande av fordon. Branschen för tunga fordon är i hög grad styrd av kostnadseffektivitet och återbetalningstid (det vill säga den tid det tar för kommersiell användning av fordonet att väga upp införskaffningskostnaden av fordonet). Extra funktionalitet för fordonet gällande bland annat säkerhetsfunktioner och däribland cybersäkerhet ökar kostnaderna och således också återbetalningstiden (Stachowski, Bielawski & Weimerskirch 2018).

3 Tidigare forskning

Detta kapitel sammanfattar tidigare forskning som utförts angående cybersäkerhet relaterat till fordon. Kapitlet fokuserar huvudsakligen på tidigare forskning som utforskat möjligheten till att utföra cyberangrepp mot fordon. Kapitlet är inte uttömmande med avseende på all forskning som utförts inom området utan tar upp väletablerad forskning med relevans för denna studie.

Syftet med kapitlet är, förutom att inkludera tidigare erhållen kunskap inom forskningsområdet, även att introducera kapitel 4, vilket diskuterar potentiella attackytor relaterat till fordon generellt och i synnerhet tunga fordon.

En majoritet av den forskning som tidigare genomförts på personfordon och tunga fordon har fokuserat på den amerikanska fordonsmarknaden. Europa och Nordamerika nyttjar i stort sett samma grundprinciper och standarder för tunga fordon. Det finns dock en del skillnader, vilka bland annat inkluderar arkitektur för trailerkommunikation (Stachowski, Bielawski & Weimerskirch 2018). I förlängningen kan detta innebära att en del av den forskning som tidigare utförts med fokus på den amerikanska marknaden inte är direkt applicerbar för den europeiska marknaden. Detta bör dock utvärderas från fall till fall. Av den tidigare forskning som inkluderats i denna studie har det inte upptäckts några uppenbara skillnader som medför att forskning inte är relevant för den europeiska marknaden.

Detta kapitel inkluderar även exempel på angrepp som utförts mot personfordon. Rapporten har tidigare diskuterat skillnader och likheter mellan personfordon och tunga fordon. Dessa skillnader rör bland annat vilken standard för den interna kommunikationsbussen som nyttjas, där personfordon nyttjar proprietära versioner av CAN och tunga fordon primärt bygger på J1939. Detta medför att angrepp som utförs mot personfordon troligtvis inte direkt kan överföras på tunga fordon och inte heller till andra personfordonsmodeller av andra tillverkare (Burakova, Hass, Millar & Weimerskirch 2016). Däremot beskriver Stachowski, Bielawski och Weimerskirch (2018) att de sårbarheter och hot som personfordon och tunga fordon kan utsättas för är mycket lika. Därför är det relevant att inkludera sådana exempel i rapporten då liknande angrepp potentiellt kan användas mot tunga fordon.

Så vitt vi vet, eller kunnat se, har det ännu inte förekommit några skarpa cyberangrepp mot vare sig tunga fordon eller personfordon. Därför finns det heller inte några beskrivningar av sådana i studien.

3.1 Hackade färdskrivare

Angreppet som berör tunga fordon är egentligen inte direkt relaterat till tunga fordon men utnyttjar sårbarheter i internetanslutna och öppna färdskrivare.

Norte (2016) genomförde sökningar i sökmotorn Shodan[6] och fann i dessa sökningar ett antal internetanslutna telematikenheter. Dessa enheter återfinns till största del i tunga fordon och samlar in data bland annat rörande fordonets position och hastighet och kan även användas för att externt ansluta till fordonets interna kommunikationsbuss. Externa anslutningar är möjliga eftersom enheterna har externa nätverksgränssnitt och genom 3G/4G kan kommunicera över internet.

Norte (2016) fann att dessa enheter sällan var skyddade mot extern anslutning och saknade lösenordsskydd, vilket specifikt gällde enheter av modell *c4max*. Dessa enheter hade även en direkt anslutning till den interna kommunikations-bussen. Av etiska skäl utförde Norte inte några ytterligare experiment med dessa enheter. Norte spekulerade dock i att angrepp på dessa enheter från distans skulle kunna få allvarliga konsekvenser.

3.2 Exempelangrepp på lastbil och buss

Burakova et al. (2016) genomförde ett antal experiment av standarden J1939 inom en icke-modifierad tung lastbil, årsmodell 2006 (klass 8 enligt amerikansk klassifikation, vilket innebär en tjänstevikt på över 15 ton) och en amerikansk skolbuss årsmodell 2001. Målet med studien var att undersöka om öppenheten i standarden J1939 kan utnyttjas för att utföra angrepp mot tunga fordon.

Genom experiment i studien visar Burakova et al. (2016) att det är möjligt att överskrida indata till gasreglaget från föraren genom att skicka falska paket. Forskarna kunde genom detta få fordonet att accelerera eller avlägsna möjligheten att förse hjulen med drivkraft. Författarna beskriver att det bästa föraren kan göra om detta inträffar är att stanna fordonet, vilket inte alltid är lämpligt.

I ett annat av experimenten som utfördes kunde Burakova et al. (2016) genom att skicka falska paket även kontrollera mätare i instrumentpanelen. Dessa inkluderade bland annat oljetemperatur, oljetryck, kylartemperatur, hastighet, bränslenivå och varvtal för motorn. När dessa mätares respektive gränsvärden överskreds skickades ett larm vilket vanligen innebär att en lampa i instrumentpanelen tänds samtidigt som ett larm ljuder.

Inget av de angreppsexempel som utförs i studien medförde direkt skada på fordonet eller omgivningen. Det är däremot rimligt att anta att en stor mängd av plötsliga varningar via ljud och lampor på instrumentpanelen tillsammans med att fordonet börjar accelerera på egen hand kan få föraren att tillfälligt tappa fokus på körningen, vägen och omgivningen vilket i sin tur kan förorsaka en olycka.

[6] https://www.shodan.io

Angreppsexperimenten utfördes primärt på den tunga lastbilen och testades sedan på skolbussen för att sedan se om angreppen kunde återanvändas utan modifikation. Resultatet var att en del av experimenten fungerade på båda fordon och andra fungerade endast på den tunga lastbilen. Studien visar att öppenheten i standarden J1939 och dess breda användningsområden kan utgöra betydande hot mot en stor mängd tunga fordon.

Burakova et al. (2016) påpekar i sin rapport att även om de i experimenten krävde fysisk tillgång till fordonen för att utföra angreppen är det rimligt att angreppen kan utföras på distans. Detta kan tänkas vara möjligt, exempelvis via internetanslutna telematikenheter som beskrevs i avsnittet om Norte (2016) ovan.

Vidare skriver Burakova et al. (2016) att deras angrepp endast tog dem två månader att implementera och utföra och krävde ingen proprietär information. Det är därför rimligt att en antagonist med mer tid kan skapa än mer sofistikerade angrepp som dessutom skulle kunna utföras på distans.

3.3 Hackad telematiktjänst

I en kortare artikel på sin hemsida beskriver Argus Cybersecurity (2020) ett angrepp på en telematiktjänst vid namn *Zubie* från en tredjepartsleverantör. Zubie beskrivs som en tjänst som bland annat möjliggör upptäckt av möjliga fel i fordonet, spårning av körvanor och delande av platsinformation till andra användare via Zubie-applikationen. Dessa funktioner möjliggörs genom att ansluta en Zubie-dongel till fordonets diagnostikuttag. Dongeln ansluter till fordonets interna kommunikationsbuss och innehåller samtidigt ett GPRS-modem för kommunikation med Zubies molntjänst.

På dongeln fann forskarna en separat fysisk port, vilken efter undersökning visade sig vara ett underhållsuttag för själva dongeln. Genom att ansluta till denna kunde forskarna sedan urskilja hur dongeln kommunicerar med Zubies kontrollserver och även se dongelns interna filer. Vidare upptäcktes att varje gång dongeln kommunicerar med kontrollservern var den öppen för konfigurationsuppdateringar från servern. Det visade sig även att all kommunikation utfördes via protokollet HTTP och inte det säkrare alternativet HTTPS. Dessutom verifierade inte dongeln kontrollserverns autenticitet. Uppdateringarna till dongeln var inte heller digitalt signerade.

Sammantaget innebär detta att en antagonist kan utge sig för att vara kontroll-servern genom att förfalska dess adress och på så sätt få dongeln att ta emot uppdateringar innehållande skadlig kod. Forskarna lyckades med ett sådant angrepp och installerade genom det en Trojan i dongeln som i princip gav dem kontroll över fordonet. I artikeln beskrivs att de kunde öppna dörrarna och påverka olika delar av instrumentpanelen, men det påpekas även att det är tänkbart att mer kritiska system så som bromsar, styrning och motor kan på-verkas. Artikeln beskriver även att ju mer avancerat fordonet är desto mer av

dess interna system styrs av datorer, vilket i sin tur möjliggör denna typ av angrepp (Argus Cybersecurity 2020).

3.4 Hackade personfordon

Två välkända studier relaterat till cyberangrepp mot fordon har producerats av Miller och Valasek (2013; 2015). Den första av dessa två studier bygger på tidigare forskning som visat att det varit möjligt att exekvera kod på distans i ECU:er via trådlösa gränssnitt som exempelvis Bluetooth eller telematikenheter. Studien visade att det under vissa förhållanden går att påverka styrning, acceleration, bromsar och displayer i fordonet. Experimenten utfördes på två olika modeller av personfordon från två olika tillverkare (Miller & Valasek 2013).

I den första studien utforskades kommunikationsbussarna i fordonen samt om och hur det gick att injicera egen kommunikation på bussarna. Detta utfördes genom att ansluta en ECOM[7]-sladd mellan *On-board Diagnostics*-II-porten (ODB) och en bärbar dator. På så sätt kunde Miller och Valasek (2013) lyssna på kommunikationsbussarna, se kommunikationen och från det börja rekonstruera protokollet.

Under denna utforskning upptäcktes ett antal problem med att injicera falska paket. Bland annat visade det sig att en del funktionalitet inte styrs direkt via kommunikationsbussen, detta gällde särskilt i de fall där en funktion var inbyggd som ett subsystem i en ECU (med andra ord har funktionen ingen dedikerad ECU). Det finns även en del inbyggda säkerhetsrelaterade funktioner, vilka kan påverka möjligheten att skicka falska paket. Miller och Valasek (2013) ger exemplet att för funktionen filhållningsassistans (eng. *Lane Keep Assist* (LKA)) ignoreras paket som indikerar att ratten bör vridas mer än 5%.

Trots problemen med injicering av falska paket lyckades Miller och Valasek (2013) hitta ett antal angrepp vilka kunde nyttjas mot båda fordonen. Dessa inkluderade bland annat mindre angrepp av icke-kritisk natur så som att förändra värdet för hastighetsindikatorn eller vägmätaren. Utöver dessa lyckades man även genomföra potentiellt mer kritiska angrepp såsom att få bromsarna att sluta fungera, stänga av alla lysen (invändigt och utvändigt), stoppa motorn och få servostyrning att sluta fungera.

Miller och Valaseks (2013) första studie möttes av kritik och generellt ointresse från fordonsbranschen som påpekade att Miller och Valaseks angreppsexempel endast var möjliga att genomföra för att de hade fysisk tillgång till fordonet för

[7] https://www.cancapture.com/ecom

att på så sett injicera sina egna CAN-paket till den interna kommunikationsbussen. Toyota meddelade att ”Vårt fokus, och hela fordonsindustrins, är att motverka angrepp från trådlösa enheter utanför fordonet. Vi anser att våra system är robusta och säkra”[8].

Miller och Valaseks (2015) nästa studie fokuserade på att visa att fordon kan angripas från distans. Studien påbörjades under 2014 med att samla in information om olika fordons interna kommunikationsarkitektur i syfte att hitta modeller med en enkel arkitektur, stor potentiell attackyta samt många avancerade fysiska funktioner. Valet landade till slut på en Jeep Cherokee av årsmodell 2014 (Miller & Valasek 2015).

Nästa steg för Miller och Valasek var att utforska den interna kommunikationsarkitekturen för fordonet, vilket bland annat visade att infotainmentsystemet var anslutet till fordonets båda nätverksbussar. Utifrån detta spekulerade Miller och Valasek (2015) om huruvida det gick att kommunicera med alla ECU:er på nätverksbussen genom att skicka datapaket från infotainmentsystemets huvudenhet. Efter vidare utforskning av infotainmentsystemet och dess tillhörande wifi upptäcktes att det fanns ett antal öppna portar, en av vilka visade sig vara ett D-Bus system med en *Inter-Process Communication*- (IPC) och *Remote Procedure Call*-mekanism (RPC) för kommunikation mellan olika processer.

Miller och Valasek (2015) upptäckte att D-Bus systemet kunde nås anonymt och dessutom att de via en tjänst i denna kunde exekvera valfri kod. Dessutom visade det sig att D-Bus systemet var bunden till alla nätverksgränssnitt, alltså även över mobilnätverk. Detta innebar att tjänsten kunde anslutas till på distans, att det gick att exekvera kod från distans och att detta även kunde göras anonymt.

Genom experimentet visade Miller och Valasek (2015) att de kunde påverka kritiska fysiska system såsom styrning och bromsar i fordonet på distans. Studien resulterade bland annat i att 1,4 miljoner fordon av samma modell som användes i experimenten återkallades av tillverkaren.

[8] Ursprungscitatet, hämtat ut Miller och Valasek (2015): “Our focus, and that of the entire auto industry, is to prevent hacking from a remote wireless device outside of the vehicle. We believe our systems are robust and secure.”

4 Potentiella attackytor

Detta kapitel beskriver resultatet av litteraturstudien genom att presentera möjliga attackvektorer, angrepp och sårbarheter relaterat till tunga fordon. Kapitlet delas in i tre avsnitt varav tre beskriver de olika attackytorna i enlighet med Checkoway et al. (2011) samt Stachowski, Bielawski och Weimerskirch (2018): Trådburen kommunikation och indirekt fysisk tillgång, Trådlös kommunikation kortdistans samt Trådlös kommunikation långdistans. Kapitlets avslutande avsnitt beskriver tidigare forskning relaterat till utförda angreppsexperiment på fordon.

Observera att avsnitten i detta kapitel inte är uttömmande för alla de angrepp och angreppstyper som kan påverka olika typer av fordon och fordonsmodeller. Istället är intentionen att ge en övergripande bild för de olika möjliga attackytor som existerar för tunga fordon. Notera även att en del angreppstyper i avsnitten nedan kan vara relevanta även för andra kommunikationstyper (avsnitt) då funktionaliteten som beskrivs kan utnyttjas på flera olika sätt. Till exempel kan OBD-II-porten utnyttjas antingen via direkt fysisk åtkomst eller på distans genom att angriparen får tillgång till en internetansluten dongel som är inkopplad i porten. Attackvektorerna placeras dock under den rubrik de främst associeras med.

Flera tidigare studier har undersökt möjligheten att påverka, framförallt person-fordon, via fysiskt tillgängliga kommunikationsgränssnitt, det vill säga via trådburen kommunikation. Dessa studier kritiserades för att experimenten krävde fysisk tillgång till fordonet. Kritiken involverade främst argument kring att om en angripare har fysisk tillgång till ett fordon kan denne utföra fysiska sabotage vilka kräver betydligt mindre kompetens, förberedelser, tid och verktyg än digitala angrepp. Det finns således bättre argument för att en angripare skulle utföra fysiska sabotage snarare än digitala om denne har fysisk tillgång till fordonet. Flera av de studier som kritiserades för detta utvecklades dock senare till att visa att samma angrepp som utförts med fysisk tillgång även kan utföras på distans (Checkoway et al. 2011; Miller & Valasek 2015).

Med ovanstående argument som grund gör denna studie en distinktion mellan direkt och indirekt fysisk tillgång till ett fordon. Studien ämnar, relaterat till den fysiska attackytan, endast inkludera angrepp eller sårbarheter vilka existerar och är möjliga att genomföra via indirekt fysisk tillgång. I detta avseende innebär indirekt fysisk tillgång att angriparen har möjlighet att angripa eller infektera enheter eller system vilka via fysiskt gränssnitt (kabel) ansluts till fordonets interna system av någon annan än angriparen själv. Ett tydligt exempel på vilken typ av enhet detta kan inkludera är mobiltelefoner, vilka frekvent ansluts till fordons interna infotainmentsystem, antingen via Bluetooth eller USB-anslutning. Mobiltelefoner ansluter i sin tur till publika nätverk via 3G/4G (även

i dagsläget via 5G i begränsad utsträckning) eller wifi. Dessa anslutningar innebär att en angripare potentiellt kan ge sig på dessa enheter på distans eller också genom fysisk tillgång. Fysisk tillgång till enheter som vid senare tillfälle ansluts till fordonet av en intet ont anande användare exkluderas således inte av distinktionen.

Trådlös kommunikation kortdistans avser distansbaserad kommunikation som nyttjar protokoll vars specificerade kommunikationsavstånd är ungefär 1–100 meter. Det maximala kommunikationsavståndet för en del av de protokoll som inkluderas i denna attackyta kan dock utökas långt över vad som specificeras i respektive standard och då även vad som kan anses normalt för protokollet. Ett sådant exempel är Bluetooth som med hjälp av diverse signalförstärkare eller under särskilda förhållanden kan utöka kommunikationsavståndet till över en kilometer, snarare än de 100 meter som standarden för Bluetooth Klass 1 specificerar (Bluetooth Special Interest Group (SIG) (u.å.)). För denna attackyta avgränsas avsnittet till att endast beskriva relevanta protokoll vars standard specificerar ett effektivt kommunikationsavstånd på cirka 400 meter, även om avståndet med hjälp av signalförstärkare eller andra verktyg kan utökas.

Den tredje och sista attackytan som beskrivs i denna studie är trådlös kommunikation långdistans. Denna attackyta inkluderar alla relevanta protokoll, vilka har ett kommunikationsavstånd av magnituden kilometer.

4.1 Trådburen kommunikation och indirekt fysisk tillgång

Följande potentiella attackvektorer kräver indirekt fysisk tillgång till fordonet. Det som avses här är att angriparen själv inte har fysisk tillgång till fordonet utan måste förlita sig på användar- eller ägarintroducerade aspekter. Dessa aspekter inkluderar exempelvis enheter i form av mobiltelefoner, tredjepartsdonglar och datorer som via fysiskt medium (sladd) ansluts till fordonet. Notera att angreppsvektorer relaterat till fysiska sabotage inte inkluderas i detta avsnitt.

Avsnitt 4.1.3 utgör tillsammans med avsnitt 4.1.5 delvis ett undantag för distinktionen till fysisk tillgång. Detta eftersom dessa avsnitt beskriver aspekter och anslutningspunkter som kan nås från fordonets utsida och som vid felaktig hantering kan utgöra en vektor som kan utnyttjas av angripare för att kompromettera fordon. Det undantag som görs gällande dessa anslutnings-punkter är i de scenarier där en angripare ansluter externa enheter via anslutningspunkterna som i sin tur går att kommunicera med från distans.

4.1.1 Diagnostikuttag (OBD-II):

En kommunikationsväg som finns i alla fordon är diagnostikuttaget, som ofta benämns OBD eller OBD-II av engelskans *On-Board Diagnostics*.

Diagnostikuttaget används för att kommunicera med ett fordons interna ECU:er och används framförallt av servicetekniker för att läsa av felkoder och meddelanden från styrenheterna. Det finns ett antal nätverksprotokoll och standarder associerade med diagnostikuttaget, bland annat definierar SAE J1979 (2017) vilka data som kan erhållas via uttaget. ISO 15031-7 (2010) specificerar hur en användare via diagnostikuttaget kan kommunicera med fordonets olika ECU:er. Av särskilt intresse här är *Mode$08* som möjliggör kontrollövertagande av en styrenhet.

För att ansluta till en ECU i syfte att exempelvis utföra diagnostik eller uppdatering krävs att ECU:n först autentiserar användaren (diagnostikverktyget). Detta görs vanligen genom ett *seed/key*-schema där ECU:n efter initial kontakt skickar en *seed* för att skapa en kryptografisk nyckel (Stachowski, Bielawski & Weimerskirch 2018). Diagnostikverktyget som försöker kommunicera med ECU:n tar emot denna seed och matar in den i en kryptografisk algoritm. Algoritmen är specifikt implementerad av tillverkaren och ska hållas hemlig eftersom dess röjande motverkar hela processen. Samtidigt som diagnostikverktyget räknar ut den kryptografiska nyckeln, gör ECU:n detsamma. Detta för att sedan kunna jämföra och verifiera resultatet som skickas tillbaka från diagnostikverktyget. Om den nyckel som verktyget skickar tillbaka till ECU:n stämmer överens med den nyckel som ECU:n själv räknade ut, kan tillgång medges. Om nyckeln inte stämmer överens nekas tillgång (Stachowski, Bielawski & Weimerskirch 2018). Implementationen av dessa typer av funktioner har dock visat sig vara sårbar för angrepp. Exempelvis lyckades Miller och Valasek (2013) rekonstruera ett diagnostikverktyg varpå de fick tillgång till säkerhetsrelaterad information och den algoritm som användes för nyckelgenerering. Genom detta kunde de sedan effektivt ansluta till, och kommunicera med, alla ECU:er i fordonet.

En del leverantörer erbjuder tredjepartssystem vilka ansluts till den interna kommunikationsbussen via diagnostikuttaget. Dessa system representeras ofta av en dongel som i sin tur kan kommunicera över publika nätverk för att förmedla information om fordonet till ägaren. Exempelvis kan detta utgöras av ett FMS från tredje part. Om dessa enheter inte skyddas på ett korrekt sätt kan en antagonist fjärransluta till systemet, dongeln, och därigenom fordonets interna kommunikationsbuss.

När fordon genomgår regelbunden service inkluderas ofta olika mjukvaruuppdateringar vilka i regel utförs genom att serviceteknikern ansluter en bärbar eller stationär dator till fordonet via OBD-II-porten. Dessa datorer är i regel vanliga Windowsbaserade system och har även normalt anslutningsmöjligheter till publika nätverk (exempelvis till internet). Det är tänkbart att IT-systemen hos servicestationer eller verkstäder utsätts för angrepp, där en angripare söker tillgång till servicedatorer. Om angriparen lyckas ta sig in i en eller flera servicedatorer kan denne sedan nyttja tillgången för att ladda in skadlig kod i

fordon när uppdateringar av mjukvara utförs under service. Ett sådant angrepp kan potentiellt få stor spridning mellan olika fordonsflottor, olika fordonstyper från olika tillverkare och modeller (Checkoway et al. 2011).

4.1.2 Fysiska multimediagränssnitt:

I moderna fordon återfinns numera flera olika typer av fysiska multimedia-gränssnitt, vilka bland annat inkluderar USB-portar, läsare för minneskort[9] och CD-spelare. De senare återfinns dock i lägre utsträckning idag än tidigare och kan vara i färd med att fasas ut då de i princip har ersatts av applikationer i mobiltelefoner eller MP3-spelare.

USB-uttag nyttjas ofta i fordon för laddning av anslutna enheter, men kan även användas för att ansluta till infotainmentsystemet, exempelvis i syfte att spela upp musik från en ansluten enhet. Checkoway et al. (2011) menar att det är tänkbart att en angripare komprometterar en mobiltelefon och installerar skräddarsydd skadlig kod i den. När mobiltelefonen sedan ansluts till fordonet, via exempelvis USB, angriper den skadliga koden fordonets infotainmentsystem.

Ett annat exempel är läsare för *Secure Digital*-minneskort (SD) vilka inom fordon kan användas för att exempelvis spela upp musik. Dessa kan utsättas för samma typ av angrepp som beskrevs angående mobiltelefoner ovan (Stachowski, Bielawski & Weimerskirch 2018).

Checkoway et al. (2011) påpekar även att dessa typer av angrepp kan uppfattas som isolerade hot men att infotainmentsystem i fordon inte ska ses som isolerade system. Många infotainmentsystem är anslutna till den interna kommunikations-bussen, vilket innebär att det via infotainmentsystemet går att nå fordonets mer kritiska ECU:er. Detta illustreras även i Miller och Valaseks (2015) studie som sammanfattas i avsnitt 3.4 och påpekas även av Stachowski, Bielawski och Weimerskirch (2018).

4.1.3 Påbyggnadsgränssnitt

Som beskrivet i inledningen av detta kapitel utgör detta avsnitt ett undantag gällande distinktionen av angriparens fysiska tillgång till fordonet.

Stachowski, Bielawski och Weimerskirch (2018) menar att påbyggnadsgränssnitt kan utgöra ett för tunga fordon unik attackyta eftersom påbyggnadsgränssnitt inte erbjuds för personfordon. Vidare behöver dessa gränssnitt i regel tillgång till fordonets interna bussnätverk. Sådana anslutningar går sällan via OBD-gräns-snittet och utgör således ett annat bussegment. Hotet för denna attackvektor kan mildras genom att påbyggnadsgränssnitt ansluts via en nätsluss för att undvika

[9] Här avses primärt *Secure Digital*-minneskort (SD).

direkt fysisk anslutning till kommunikationsbussen (Stachowski, Bielawski & Weimerskirch 2018).

4.1.4 12-voltsuttag

12-voltsuttag är vanligt förekommande inom fordon och så även inom tunga fordon. För tunga fordon kan dessa uttag dock utgöra ett unikt hot eftersom elnätskommunikationen mellan dragfordon och släp (eng. *Power Line Communication* (PLC)) går via fordonets 12-voltssytem (Stachowski, Bielawski & Weimerskirch 2018). Det är enligt dem tänkbart att en angripare med hjälp av skadlig kod komprometterar en användarenhet som nyttjar 12-voltsström och inbäddad PLC-hårdvara. När enheten sedan ansluts till ett 12-voltsuttag i fordonet börjar den att modulera signaler som stör funktionen hos de ECU:er som använder PLC-protokollet.

4.1.5 Elnätskommunikation för dragfordon och släp

Trailers och släp för tunga fordon behöver kommunicera med dragfordonet. Inom EU används den CAN-baserade ISO 11992-standarden vilken specificerar parametrar för bromssystem, styrning, fjädring och hjul. Stachowski, Bielawski och Weimerskirch (2018) beskriver att nyare tunga fordonsdesigner i Europa kan inkludera ett antal olika anslutningsgränssnitt bland annat, ISO 12098, ISO 7638, ISO 1185 och ISO 3731.

Det primära problemområdet för dessa gränssnitt är att en angripare kan utnyttja de fysiska anslutningspunkterna för elnätskommunikationen vilka är exponerade längs släpets ram. På samma sätt som beskrivits i avsnitt 4.1.4 kan modulerade signaler skickas över 12-voltskanalen för att störa funktionen hos ECU:er som nyttjar PLC-protokollet. Detta kan i sin tur påverka funktionen hos exempelvis bromssystem och styrning för släpet.

4.2 Trådlös kommunikation kortdistans

Denna kategorisering av attackvektorer involverar trådlös kommunikation som utförs på kort distans.

4.2.1 Bluetooth

Bluetooth[10] och andra kortdistansprotokoll kan numer ses som en standard-funktionalitet i fordon och används vanligen för att ansluta mobiltelefoner eller

[10] Notera att det vid ett flertal tillfällen har visats att Bluetooth-kommunikation kan förlängas långt över de 100 meter för klass 1 som standarden beskriver (Bluetooth Special Interest Group (SIG) (u.å.)). Även

andra mobila enheter för användning i fordonets infotainmentsystem. Bluetooth kan även enligt Stachowski, Bielawski och Weimerskirch (2018) nyttjas för *Over-The-Air*-uppdateringar (OTA).

Miller och Valasek (2015) påpekar att det primärt finns två olika angrepps-möjligheter för Bluetooth. Den första och potentiellt mest skadliga involverar en icke-parad enhet och den andra involverar att utnyttja en redan parad enhet. Den andra möjligheten utgör enligt Miller och Valasek (2015) ett mindre hot eftersom den kräver interaktion från användaren.

4.2.2 Wifi

Det är numer vanligt för personfordon att erbjuda internetanslutning via 3G/4G-modem i fordonet som sedan bryggas mot passagerares enheter genom att agera *hotspot*. Tunga fordon nyttjar även wifi-anslutningar, men ofta för andra ändamål, specifikt för diagnostik och logistik (Stachowski, Bielawski & Weimerskirch 2018).

Miller och Valasek (2015) fann öppna portar via det undersökta fordonets wifi, vilka användes av fordonets infotainmentsystem. I studien lyckades man komma åt och exekvera godtycklig kod i fordonets infotainmentsystem via en öppen port för en D-bus tjänst. Miller och Valasek (2015) visade även hur de kunde röra sig lateralt via D-bus systemet och skicka valfria CAN-paket för att påverka andra system i fordonet.

Wifi i sig är en mogen standard och erbjuder relativt robust säkerhet via *Wi-Fi Protected Access version 2*-kryptering (WPA2)[11]. Miller och Valasek (2015) lyckades dock knäcka det slumpmässiga lösenordet mycket snabbare än vad som egentligen är möjligt i en uttömmande sökning på grund av en sårbarhet i implementationen för hur lösenord genererades.

Det bör dock noteras att räckvidden för wifi ligger i paritet med Bluetooth klass 1 och begränsar således möjligheterna för ett angrepp från distans.

4.2.3 Tire Pressure Monitoring System

Tire Pressure Monitoring System (TPMS) har implementerats i alla personfordon i USA sedan 2008 (enligt FMVSS 138) och sedan 2014 inom EU (numer enligt UN ECE R141). TPMS används även inom den tunga fordonsindustrin men är

om detta är möjligt, kategoriseras Bluetooth som ett kortdistansprotokoll i denna rapport eftersom detta är vad standarden specificerar.

[11] WPA2 har börjat ersättas av den nyare och säkrare WPA3-standarden.

ännu inte lagstadgat. EU har dock beslutat att revidera den allmänna säkerhets-föreskriften till att bland annat inkludera TPMS-krav för tunga fordon (ETRMA 2019).

Dessa system nyttjar vanligen Bluetooth eller andra protokoll för trådlös kommunikation för att kommunicera data angående nuvarande lufttryck i däcken till fordonets interna kommunikationsbuss. Eftersom status för TPMS normalt visas i en av fordonets instrumentpaneldisplayer menar Stachowski, Bielawski och Weimerskirch (2018) att TPMS-signalmottagaren med stor sannolikhet är ansluten till den interna kommunikationsbussen (eller integrerad i en annan ECU). På så sätt kan mottagaren även skicka datapaket över kommunikationsbussen till instrumentpanelen som i sin tur visar information om nuvarande däcktryck.

Enligt Miller och Valasek (2015) är det möjligt att påverka TPMS, exempelvis för att få fordonet att tro att det har ett problem med däcken. Stachowski, Bielawski och Weimerskirch (2018) spekulerar i att en komprometterad TPMS-mottagare kan injiceras med skadlig kod som senare sänder ut felaktiga paket på kommunikationsbussen. Det har även visat sig vara möjligt att krascha och effektivt förstöra den TPMS-associerade ECU:n i ett fordon (Metzger 2010).

4.2.4 Remote Keyless Entry System

Remote Keyless Entry-system (RKE) erbjuder funktioner för att kunna låsa och låsa upp dörrar, kontrollera belysning och att starta motorn från distans. Dessa funktioner är vanliga i både personfordon och tunga fordon, även om det för tunga fordon erbjuds färre funktioner (Stachowski, Bielawski & Weimerskirch 2018). Vanligen implementeras dessa system i någon slags fjärrkontroll eller nyckeldosa, men det är numer även vanligt att samma funktionalitet erbjuds via applikationer i mobiltelefoner.

RKE nyttjar ofta någon form av kryptering i syfte att motverka att en angripare snappar upp signaler som denne sedan själv kan använda för att få tillgång till fordonet. Enligt Stachowski, Bielawski och Weimerskirch (2018) kräver dessa system normalt en anslutning till den interna kommunikationsbussen i syfte att aktivera de funktioner som erbjuds via RKE-systemet. Trots kryptering har det vid ett flertal tillfällen demonstrerats inom såväl forskning som verklighet att RKE-system är sårbara för angrepp, bland annat i Garcia, Oswald, Kasper och Pavlidès (2016). En angripare kan via dessa angrepp få tillgång till fordonet för att exempelvis stjäla eller manipulera det. Miller och Valasek (2013) påpekar dock att attackytan för fjärrkörning av kod via RKE-system är begränsad och att ett sådant angrepp sannolikt är ogenomförbart.

4.2.5 RFID-nycklar

Personfordon har redan under lång tid varit utrustade med *Radio-Frequency Identification*-nycklar (RFID) i syfte att försvåra stöld av fordon. Nycklarna kan implementeras med antingen passiv eller aktiv transponderteknik. Det blir allt vanligare med aktiva system i och med att allt fler fordon tenderar att ha en elektronisk startknapp snarare än ett fysiskt tändningslås. När startknappen trycks in i syfte att starta fordonets motor skickas en RF-signal ut från fordonet. Signalen ska därefter plockas upp av transpondern i nyckeldosan, som i sin tur svarar med sitt unika ID. Om fordonet inte får ett korrekt ID som svar kommer motorn inte att starta. RFID-nycklar utgör således en form av elektronisk startspärr för fordonet.

Stachowski, Bielawski och Weimerskirch (2018) så väl som Miller och Valasek (2013) beskriver att det troligtvis finns få möjligheter för en angripare att via en sårbarhet i RFID-implementationen angripa den interna kommunikationsbussen och att ett sådant angrepp troligtvis endast leder till att angriparen kan inaktivera startspärren.

4.3 Trådlös kommunikation långdistans

Denna kategorisering av attackvektorer involverar trådlös kommunikation som utförs på lång distans.

4.3.1 3G/4G/5G

Många moderna fordon erbjuder numera anslutningsmöjlighet till publika nätverk via mobila nätverksmodem som placeras i fordonet och som ansluts till infotainmentsystemet.

Det fordon som Miller och Valasek (2015) utförde sina experiment på hade i tillägg till wifi även ett mobilmodem anslutet till infotainmentsystemet. Infotainmentsystemet hade i sin tur anslutning till fordonets två interna kommunikationsbussar och kunde kommunicera över dessa. Miller och Valasek (2015) visade att de utöver att kunna kommunicera med och påverka fordonet över 3G/4G med hjälp av en *femtocell,* även att de kunde kommunicera med och påverka fordonet via vilken mobilmast som helst i hela USA.

Hotnivån för denna attackvektor varierar beroende på hur mobilnätverk integreras i fordonet, med vilka ECU:er och vilka kommunikationsbussar som dessa har tillgång till. Det ska även noteras att en majoritet av de telematik-enheter som nyttjas i fordon använder någon form av mobilnätverk för kommunikation på distans. Om dessa är öppna och tillgängliga som i fallet med Norte (2016) och dessutom har en direktanslutning till de interna kommunikationsbussarna kan detta få påtagliga konsekvenser för fordonet. Särskilt om telematikenheten i fråga har bristande säkerhet, till exempel i form

av avsaknad av autentisering. Att fordon över huvud taget potentiellt kan påverkas från distans över publika nätverk utgör ett av de allvarligaste hoten mot dem och det bör vara en prioritet för fordonstillverkare att motverka sådana möjligheter.

4.3.2 Over-the-air-uppdateringar

Distansuppdateringar via OTA är en relativt ny teknik inom fordonsbranschen. Tekniken har i dagsläget en begränsad spridning inom den tunga fordonsbranschen där de flesta fortfarande utför uppdateringar via fysiska anslutningar. Användningen av OTA förväntas dock öka då det finns stora fördelar med tekniken, framför allt gällande tunga fordon. Exempelvis möjliggör OTA att diagnostik och uppdateringar kan utföras på fordon som brukas långt ifrån närmsta servicepunkt. Detta innebär i sin tur en kostnadseffektivitet för ägaren eftersom det potentiellt ökar drifttiden för fordonen. Samtidigt påpekar Stachowski, Bielawski och Weimerskirch (2018) att fordonsindustrin är medvetna om att uppdateringar och diagnostik av fordon i drift potentiellt kan äventyra fordonssäkerheten. Det är exempelvis tänkbart att en angripare lyckas få fordon att ta emot en skadlig uppdatering från distans. Detta lyckades Miller och Valasek (2015) med, även om detta vid tillfället utfördes med hjälp av fysisk tillgång.

4.3.3 FMS och telematiksystem

I avsnitt 3.3 visas att det är möjligt att framgångsrikt angripa FMS och telematiksystem på distans. Konsekvenserna av ett framgångsrikt angrepp mot dylika system beror på implementationen av systemen och om de har anslutits till den interna kommunikationsbussen. Stachowski, Bielawski och Weimerskirch (2018) beskriver att så ofta är fallet, vilket kombinerat med att telematiksystem ofta fokuserar på funktionalitet snarare än säkerhet kan innebära att fordon utsätts för påtagliga risker att påverkas på distans.

Utöver påverkan visade även Norte (2016) att det finns integritetsrelaterad problematik med öppna telematikenheter som bland annat innebar att det gick att ta fram GPS-position för fordon. Detta skulle exempelvis kunna nyttjas för att förfölja ett fordon i syfte att stjäla lasten.

4.3.4 Sensorer

Nyare fordon, och i synnerhet tunga fordon, nyttjar en mängd olika sensorer, exempelvis för LIDAR, GPS, kameror och radar. Stachowski, Bielawski och Weimerskirch (2018) kategoriserar två angreppstyper mot sensorer, förfalskning och tillgänglighetsangrepp (eng. *Denial-of-Service* (DoS)). De beskriver även att systemen som använder sensorerna ofta ansluts till telematiksystemet, vilket i sin

tur har en anslutning till den interna kommunikationsbussen. Således utgör angrepp mot sensorsystem även en attackvektor för den interna kommunikationsbussen.

5 Säkerhet i fordon

Traditionell fordonssäkerhet har fokuserat på den aspekt som i det engelska språket benämns som *safety*. Begreppet safety har ingen direkt översättning till svenska, utan ingår som en del i begreppet säkerhet. Det är dock relevant att skilja dessa begrepp åt för att förstå hur säkerhet i fordon har utvecklats med tiden. Safety kan närmast förklaras som säkerhet som rör människor eller miljö och skyddet av dessa mot icke-antagonistiska hot. Termen *personsäkerhet* kommer därför att användas för att beteckna safety i resten av rapporten.

5.1 Personsäkerhetsfunktioner

Sedan T-Ford modellens introduktion år 1908 har det skett många säkerhetsmässiga förbättringar och uppfinningar i motorfordon. Dessa inkluderar bland annat introduktionen av trepunktsbältet, krockkudden och deformationszoner. Under denna drygt hundraåriga period har det fallit naturligt att fokusera på de aspekter av säkerhet som gynnar skyddandet av människan. Detta stämmer även idag, men i och med att motorfordon idag är långt mer komplicerade och avancerade än förut, samt att de i allt större utsträckning ges nätverksanslutningsförmåga har det blivit en nödvändighet att inkludera cybersäkerhet för att erhålla och bibehålla adekvata personsäkerhetsnivåer.

Personsäkerhetsfunktioner har ofta även positiva effekter för cybersäkerhet. Ett exempel på detta kan hämtas från Miller och Valaseks (2013) studie där det för många funktioner de testade att utnyttja fanns inbyggda begränsningar i när de kunde användas. Exempelvis gällde detta för experimenten med avtappning (eng. *bleeding*) av bromsarna, vilket resulterar i att bromsarna slutar fungera. Detta kunde endast utföras i stillastående läge eller vid en maxhastighet av drygt 8 km/h.

Miller och Valasek (2013) beskriver även andra personsäkerhetsfunktioner, vilka ur den studiens synsätt beskrivs som problem. Även om en angripare lyckas identifiera och rekonstruera viktiga CAN-paket via kommunikationsbussen, för att sedan använda och skicka dessa själv är det inte säkert att detta kommer att få en effekt. En av anledningarna till detta är att ECU:n som i normala fall är avsändaren av dessa paket fortfarande kommer att kommunicera dessa paket till mottagaren. Detta sker samtidigt som angriparen skickar de falska rekonstruerade paketen med samma ID, men med annat innehåll. Detta kan innebära att man som angripare måste skicka en konstant ström av paket för att dölja den legitima kommunikationen och på så sätt få en ihållande effekt. I vissa fall kan detta leda till att den mottagande ECU:n tolkar detta som ett fel i systemet och slutar lyssna på paketen som skickas, således fås ingen effekt alls (annat än att funktionen slutar fungera och förhoppningsvis går över i felsäkert läge).

Andra funktioner kan innehålla gränsvärden för vad som är möjligt att utföra. I avsnitt 3.4 beskrevs hur LKA-systemet för en av modellerna som testades i studien endast tillät ett rattutslag på mindre än 5 %, vilket innebär att alla paket som specificerade en vridning högre än detta ignoreras.

5.2 Konventionella IT-säkerhetsfunktioner

Utöver inbyggda personsäkerhetsfunktioner med positiva effekter för fordons cybersäkerhet finns även specifika cybersäkerhetsfunktioner. Dessa funktioner baseras till stor del på konventionella säkerhetsfunktioner som normalt nyttjas i datorsystem, men som av diverse anledningar inte direkt kan appliceras inom fordon. I detta avsnitt beskrivs ett antal utvalda säkerhetsfunktioner, varför konventionella säkerhetsfunktioner inte med lätthet direkt kan appliceras inom fordon samt hur säkerhetsfunktioner kan modifieras för att appliceras inom fordon.

Säkerhetsfunktioner som normalt används inom datorsystem och nätverk kan inte med lätthet appliceras inom fordon, särskilt inte för säkerhetskritiska funktioner med höga krav på realtidskommunikation. Ett exempel på detta är traditionella autentiseringsfunktioner. De interna kommunikationsbussarna för fordon implementeras i en bredsändningsstruktur där alla enheter sänder kommunikation som kan uppfattas av alla andra enheter på kommunikationsbussen. Detta innebär även att vilken enhet som helst som ansluts till bussen kan maskeras som en legitim ECU och sända falska paket som uppfattas av andra legitima ECU:er.

Autentiseringsfunktioner framstår som en god lösning på problemet med bredsändning, men kan dock inte med lätthet implementeras i fordon. Detta beror bland annat på att J1939-paket i regel endast tillåter en nyttolast om 8 byte, vilket lämnar mycket lite utrymme för meddelandeautentisering. Ett annat problem är effekterna som autentiseringsfunktioner har på tidsfördröjning av kommunikation (eng. *latency*) vilket ofta, särskilt för funktioner med höga realtidskrav, innebär att sådana funktioner helt enkelt inte kan accepteras (Stachowski, Bielawski & Weimerskirch 2018).

Det finns dock delar av fordonsinfrastruktur som kan använda, och kan gynnas av att använda, konventionella IT-säkerhetsfunktioner. Det finns även anpassade metoder och funktioner att tillgå för användning i de delar av fordon som inte kan nyttja konventionella IT-säkerhetsfunktioner. Detta avsnitt ämnar beskriva ett urval av sådana metoder och funktioner med fokus på cybersäkerhetsskydd av fordon ur ett holistiskt perspektiv.

5.2.1 Segmentering

OBD-II-portar har länge ansetts vara säkra eftersom det endast varit service-tekniker som har haft tillgång till verktyg för att använda dem, vetat hur de

används och var de finns. På senare år har det dock blivit allt vanligare att konsumenter köper OBD-donglar med trådlösa gränssnitt. Dessa donglar har designats för att vara lätta att använda och implementerar sällan adekvata säkerhetsfunktioner. Detta har lett till att OBD-II-porten nu och framöver troligtvis kommer förses med en nätsluss eller brandvägg av tillverkaren i syfte att begränsa möjligheterna för en dongel att påverka fordonets interna kommunikation (Stachowski, Bielawski & Weimerskirch 2018).

Stachowski, Bielawski och Weimerskirch (2018) beskriver även att infotainmentsystem är i färd med att segmenteras från de mer kritiska kommunikationsbussarna. Samtidigt påpekas att infotainmentsystem i en del fall spänner över flera ECU:er på olika nätverksbussar och därför saknar en tydlig gräns, vilket försvårar segmentering. I dessa fall kan det därför krävas en omstrukturering av nätverksbussarna och vilka ECU:er de inkluderar i syfte att effektivt segmentera system. En sådan segmentering skulle exempelvis ha kunnat försvåra Miller och Valaseks (2015) experiment med att via infotainment-systemet påverka cyberfysiska system i fordon.

5.2.2 Avvikelseupptäckt

Miller och Valasek (2013) beskriver att deras angrepp är relativt enkla att upptäcka eftersom alla involverar att skicka nya och ovanliga CAN-paket eller att översvämma kommunikationsbussen med vanligt förekommande paket. Till exempel samlade Miller och Valasek (2013) in kommunikationsdata under 22 minuter i ett av fordonen samtidigt som de utförde standardfunktioner (starta motor, stanna motorn, körning, bromsning och så vidare). Under denna period samlades inga diagnostiska datapaket in, vilket innebär att förekomsten av dessa typer av datapaket under normalt bruk av fordonet är en indikator på att något är fel.

Sådana indikatorer skulle kunna nyttjas av intrångsdetekteringssystem (eng. *Intrusion Detection/Prevention System* (IDS/IPS)) som föreslås av Stachowski, Bielawski och Weimerskirch (2018). Ett IDS upptäcker avvikelser i IT-system med hjälp av till exempel maskininlärning eller heuristik, eller via aktiv kommunikationsfiltrering i en nätsluss.

Stachowski, Bielawski och Weimerskirch (2018) beskriver att personfordons-industrin är i färd med att undersöka möjligheterna av att implementera IDS i personfordon. Sådana system är även möjliga att nyttja inom tunga fordon eftersom CAN och J1939 har många likheter på de lägre nivåerna i OSI-modellen. Däremot uppfattar Stachowski, Bielawski och Weimerskirch (2018) att det kan bli svårare att framgångsrikt implementera IDS i tunga fordon eftersom nätverksstrukturen är mer dynamisk än den hos personfordon. Detta baseras på att moduler i tunga fordon utför adressanspråk när modulerna startar. Detta innebär att nya J1939-moduler från tredje part som installeras i fordonet

kommer skapa en ny adress när denna startar och då förändra kommunikationslandskapet (Stachowski, Bielawski & Weimerskirch 2018).

Föreslagna modeller för IDS inom fordon ämnar skapa en referensmodell för en relativt statisk fordonsarkitektur, där all busstrafik under naturliga förhållanden lärs in för att sedan kunna upptäcka avvikelser. Den statiska arkitekturen lämpar sig väl för personfordon eftersom att arkitekturen hos personfordon sällan förändras efter att fordonet tagits i bruk. Detta innebär att IDS kan kalibreras redan i fabriken. För tunga fordon blir detta svårare eftersom fordonen ofta genomgår förändringar efter fabriksproduktion, där tredjepartsenheter ofta läggs till vid senare tillfällen (Stachowski, Bielawski & Weimerskirch 2018).

5.2.3 Säkerhetshårdvara

Säkerhetshårdvara, från engelskans *Hardware Security Module* (HSM), är fysiska kryptografiska processorer, vilka utför kryptografiska beräkningar och lagrar känslig information så som kryptografiska nycklar. En annan aspekt av HSM som är synnerligen relevant för resursbegränsade system är att de kan utföra kryptografiska beräkningar mycket snabbare än mjukvara, vilket minskar fördröjning av kommunikation. Som tidigare beskrivet i avsnitt 5.2 är fördröjning av kommunikation en anledning till att säkerhetsfunktioner så som kryptering eller autentisering inte kunnat accepteras i en del tidskritiska system inom fordon.

5.2.4 Nyckelhantering och autentisering

Ett problem som nyckelhanteringsprocessen seed/key, som vanligen används inom diagnostiska verktyg för fordon, är att nödvändig säkerhetsinformation lagras lokalt i verktygen. Detta medför att en angripare med tillräcklig kunskap för att rekonstruera verktyget kan få tillgång till säkerhetsinformation som denne sen kan använda för att producera egna legitima nycklar. Detta visades bland annat av Miller och Valasek (2013).

6 Intervjuer

Detta avsnitt presenterar resultaten från de intervjuer som genomförts i studien. Resultaten redovisar en sammanställning av de resonemang som bedömts ha störst betydelse för studiens resultat. Avsnittet struktureras efter identifierade kategorier vilka uppkommit genom intervjuerna. Innehållet som beskrivs i dessa avsnitt presenterar resonemang från olika intervjuade individer. Vid specifika resonemang eller citat benämns respondenterna som ”[resp. x]”, där x = *1, 2…,5*.

Intervjuerna i studien påbörjades under hösten år 2020 med start den 13 oktober. Som tidigare beskrivet i avsnitt 1.2 genomfördes totalt fem intervjuer med fem individer från fyra olika organisationer. Fyra av respondenterna arbetar inom räddningstjänsten i olika delar av landet. En av respondenterna arbetar för en tillverkare av tunga fordon.

På grund av den globala Covid-19-pandemin har det inte varit möjligt att genomföra intervjuer genom personliga möten på sedvanligt sätt. Istället har alla utom en intervju genomförts över telefon och en intervju via ett videokonferens-system.

6.1 Medvetenhet vad gäller cybersäkerhet i fordon

Att döma av respondenternas resonemang kring cybersäkerhet i fordon är cybersäkerhetsmedvetenheten bland brukare och ägare av tunga fordon relativt låg. Respondenterna upplever att ämnet sällan, om ens någonsin, diskuteras i relation till fordon, vare sig internt, med leverantörer eller i andra sammanhang som berör fordon.

> *Upplever inte att man pratar om cybersäkerhet, i alla fall inte i relation till fordonen* [resp. 3].

Det framkommer även att det inte finns någon uttalad cybersäkerhetsprocess i samband med inköp av fordon eller användandet av dem. Däremot finns informationssäkerhetsprocesser och rutiner för vanliga datorsystem i kontorsmiljö. Det är därför möjligt att hela processer och rutiner eller delar av dessa även nyttjas i relation till fordonen vare sig medvetet eller omedvetet. Vilket i sin tur kan medföra positiva effekter för fordonens säkerhet. Dessa processer hanteras dock av andra organisationsdelar än vad de individer som intervjuats ingår i.

En av respondenterna [resp. 5] uttryckte att denne gärna ser myndighetsinitierade riktlinjer för cybersäkerhet i relation till tunga fordon.

6.2 Beställningsprocess och granskning av leverantörer och utbud ur cybersäkerhetssynpunkt

Majoriteten av respondenterna uppger att de inte granskar påbyggnads-leverantörer av tunga fordon eftersom det endast finns två stora leverantörer i landet gällande tunga fordon för räddningstjänsten. De berättar även att det inte sker någon kravställning med avseende på cybersäkerhet i fordonen. Det finns dock en del ramavtal[12] för fordon och annan relevant utrustning, dessa nyttjas dock främst av storleksmässigt mindre räddningstjänster.

Räddningstjänsterna har själva möjlighet att bestämma innehållet i fordonen med avseende på utrustning undantaget en del system som är relevanta för Rakel-systemet. Således kan fordon hos räddningstjänster från olika kommuner innehålla olika utrustning, vilket i sin tur kan innebära olika cybersäkerhets-mässiga konsekvenser för fordonen. Exempelvis kan detta innebära att ett angrepp som utnyttjar ett specifikt påbyggnadssystem eller enhet som nyttjas av en räddningstjänst inte nödvändigtvis kommer att vara framgångsrikt mot fordon från andra räddningstjänster.

6.3 Service och uppdatering

Räddningstjänster i olika kommuner har olika rutiner för service av fordon och utrustning. I en del fall sköter stationen i fråga eller kommunen all service själva. I andra fall utförs service av fordonets grundkonstruktion av tillverkaren samt av påbyggnadsleverantören, vilka skickar servicetekniker för regelbunden service någon gång per år. Vidare kan uppdateringar av vissa system ske på distans genom att leverantören fjärransluter till stationen och till specifika fordon. I de fall när fjärranslutning kom på tal under intervjuerna påpekades även att dessa uppdateringar inte kan utföras vid godtycklig tidpunkt av leverantören utan det krävs initiering av ansvarig personal på räddningstjänstens station för att uppkoppling ska ske.

Ovanstående utsagor liknar OTA-uppdateringar, men skiljer sig på en viktig punkt, nämligen att fordonen själva inte har någon anslutningsmöjlighet till publika nätverk undantaget när de är på stationen. Under andra intervjuer fram-kom att det fanns möjlighet för OTA-uppdateringar, men att de i dagsläget är mycket begränsade. Exempelvis är det endast vissa system som kan ta emot sådan uppdatering och vidare kan dessa uppdateringar inte utföras godtyckligt av leverantören, delvis för att motverka att fordonssystem försöker uppdatera under

[12] Se exempelvis MSB:s BAS-bilsprogram https://www.msb.se/sv/amnesomraden/skydd-mot-olyckor-och-farliga-amnen/raddningstjanst-och-raddningsinsatser/bas-bil/ [2020-11-16]

pågående utryckning. En respondent [resp. 2] berättade att påbyggnads-leverantörer för vissa system har möjlighet att ansluta till systemen från distans i syfte att kunna avläsa fel och utföra mindre justeringar. Slutligen uppgav en respondent [resp. 1] att det i nuläget inte finns möjlighet för OTA-uppdateringar men att detta kan bli relevant i framtiden.

En respondent [resp. 4] som kommer från tillverkarsidan (benämns i texten som tillverkarrespondenten) uppgav att det finns möjlighet för OTA-uppdateringar, men att detta beror på vilken version av telematikenhet som fordonet har. Vidare är det bara vissa system som kan uppdateras på detta sätt. Samtidigt uppgavs att man i nuläget även bygger ut möjligheten för OTA-uppdateringar, men att utvecklingen sker långsamt eftersom det finns många risker. Som exempel på en sådan risk utrycktes att en angripare kan lyckas få fordon att ta emot angriparens egen uppdatering och således medge tillgång och påverkan på fordonet för angriparen.

En respondent [resp. 1] uttryckte att de försöker hålla alla fordon så lika som möjligt för att behålla en homogenitet i fordonsflottan. Samme respondent angav även att man helst inte vill ta emot nya uppdateringar från leverantörer utan väntar gärna några månader tills det att uppdateringen testats ordentligt i verkligheten (av andra).

6.4 Redundans

Alla fordonens system har någon form av redundans, som exempel angavs att om GPS-systemet slutar fungera så finns det fysiska kartor att tillgå. Det ska noteras att denna redundans inte fullt ut inkluderar fordonets grundkonstruktion, till exempel motor, bromsar och styrning.

Vidare uppgav flera respondenter att de nyttjar en separat bärbar dator i fordonen, vilken bland annat används för uppslag i databaser och tillgång till verksamhetssystem. Redundans för denna dator fås genom att verksamhets-systemet (vilket utgör den bärbara datorns primära funktion) även finns tillgängligt via personalens mobiltelefoner.

> *Systemen är till för att underlätta insatser, men insatser ska kunna utföras framgångsrikt oavsett* [resp. 3].

Redundanta system kan få sekundära, men positiva, effekter på cybersäkerheten eftersom det blir svårare för en potentiell angripare att åsamka bestående negativa effekter på fordonets funktion.

6.5 Fordons ålder, kostnad och livscykel

Respondenterna uppger att medelåldern för räddningstjänstsfordon i Sverige är drygt 10-15 år. Det påpekas även att det inte är ovanligt med fordon som är 20 år eller äldre.[13]

Tunga fordon inom räddningstjänsten kostar 4-8 miljoner kronor. Den stora investering som ett nytt fordon innebär kan delvis förklara varför fordon används så länge. En annan aspekt att hänsyn till är att slitaget på fordonen generellt är mycket lågt då de sällan körs långa sträckor, vilket i sin tur innebär att fordonen är i brukligt skick mycket längre än fordon inom andra användningsområden. Dessutom sköts och servas fordonen mycket noggrant.

Några respondenter uppger att de uppdaterar äldre fordon med ny teknik så långt det går, vad detta avser specifikt framgick inte alltid, men en respondent [resp. 5] uppgav att den teknik som uppdaterades främst rörde egna system och enheter utöver påbyggnadskonstruktionen. Det påpekades exempelvis att äldre fordon mycket sällan byggs om för att uppdatera fysiska system så som släcksystem. Nya fordon är generellt att föredra eftersom de innehåller nyare teknik, både i grundkonstruktionen och i påbyggnaden.

6.6 Anslutningsmöjligheter och sårbarheter

En respondent [resp. 1] uppgav att man har tagit bort alla anslutningsmöjligheter i fordonen när de är utanför stationen. Andra respondenter berättade att de har mobila bredband i fordonen för att den bärbara dator som finns i fordonen ska förses med anslutningsmöjligheter och kunna göra uppslag i centrala databaser. Majoriteten av respondenterna uttryckte att de har vanliga bärbara datorer i fordonen, en del har även andra enheter som exempelvis surfplattor. För sådan utrustning som varken tillhör fordonet eller påbyggnadsleverantören ansvarar den egna (kommunens) IT-avdelning för säkerhet och uppdatering.

En del påbyggnadsinstallationer är inkopplade på de interna kommunikations-bussarna och har samtidigt publika anslutningsmöjligheter. Tillverkar-respondenten uppger att påbyggnadinstallationer alltid ska anslutas till de interna kommunikationsbussarna via ett särskilt gränssnitt.

Vilka sårbarheter som upplevs av respondenterna varierar, vilket delvis kan ha sin förklaring i olika kompetensområdesfokus. De flesta uppgav dock att den attackyta de ansåg som mest trolig var direkt fysisk interaktion[14] med fordonet, det vill säga att en angripare har fysisk tillgång till fordonet för att exempelvis utföra sabotage . Tillverkarrespondenten uppgav dock att de inte ser några

[13] Det äldsta fortfarande aktiva fordonet sammantaget över alla intervjuer var 30 år gammalt.

[14] Av alternativen direktkontakt, närhet eller på avstånd

utbreda hot mot tunga fordon med undantaget för olika former av tillgänglighets-angrepp.

Tillverkarrespondenten angav ett exempel på DoS-angrepp i form av utnyttjande av *geofence*-regler. Geofencing är ett sätt att geografiskt avgränsa specifika områden och inom dessa områden specificera olika regler för exempelvis ett fordons beteende. Med detta som bakgrund skulle det exempelvis vara möjligt att sätta hela Sverige som ett geofence-område. En angripare skulle då sedan kunna sätta en maximalt tillåten hastighet för fordon inom området till 5 km/h, resultatet av detta blir då en form av DoS-angrepp. Detta kan i sin tur medföra stora konsekvenser beroende på hur många, och vilka typer av, fordon som påverkas av angreppet. Tillverkarrespondenten påpekade dock även att föraren har möjlighet att åsidosätta regleringen vid behov.

Nya fordon har relativt många ECU:er som agerar i en decentraliserad miljö. Tillverkarrespondenten ser att i framtiden kommer utvecklingen gå mot en centraliserad arkitektur med färre, men mer kraftfulla ECU:er. Detta leder i sin tur till att det finns ett större utrymme att inkludera säkerhet direkt i ECU:erna, eftersom de har beräkningsförmåga och resurser nog att hantera säkerhets-funktioner och säkerhetshårdvara. Samtidigt påpekas att en sådan utveckling innebär att individuella ECU:er, och i förlängningen fordonet, blir mer känsliga för uppkomsten av fel. Detta eftersom varje individuell ECU kommer att hantera och styra mer av fordonets funktionalitet.

Tillverkare av tunga fordon är väl medvetna om att tredjepartsprodukter ofta inkluderar en mobil internetanslutning, vilken kan utnyttjas av potentiella angripare. Det är därför viktigt att tillverkaren begränsar vilka data som är möjliga att hämta ut via de gränssnitt till vilka dessa tredjepartsprodukter ansluts.

Vissa påbyggnadsinstallationer kräver tillgång till de interna kommunikations-bussarna för att fungera på ett korrekt sätt. Exempelvis behöver en del påbyggnader tillgång till, och kontroll över, fordonets motor i syfte att förse påbyggnaden med tillräcklig kraft för att kunna verka. Sådan kontroll utförs genom att påbyggnaden skickar kommandon vilka överförs till de interna kommunikationsbussarna via ett särskilt påbyggnadsgränssnitt. Vilka kommandon som påbyggnader har tillåtelse att skicka och som skickas vidare till de interna kommunikationsbussarna bestäms genom vitlistning i gränssnittet. Det är dock möjligt att byta ut mjukvaran i gränssnittet för att bestämma en egen godtycklig vitlistning, men detta kräver fysisk tillgång till fordonet.

7 Diskussion

Detta kapitel presenterar en diskussion kring intervjuernas resultat, kombinerat med resultaten från litteraturstudien, i relation till studiens fyra huvudfrågeställningar.

7.1 Urvalets påverkan på resultatet

Studiens huvudfrågeställningar är relativt spridda, i bemärkelsen att de täcker olika kunskapsområden. Intervjuernas frågeställningar ämnar bryta ner studiens huvudfrågeställningar i mer specifika och konkreta frågor, vilket i sin tur har ökat spridningen. Detta har i sin tur inneburit att det varit svårt för en specifik arbetsroll eller individ att besvara samtliga frågor, vilket i sin tur har påverkat mängden respons för varje intervjufråga och i förlängningen även för studiens frågeställningar.

Urvalet av respondenter har präglats av den under år 2020 rådande situationen med covid-19 och de restriktioner och rekommendationer som getts av Folkhälsomyndigheten. Situationen har bland annat inneburit att det inte varit möjligt, eller i alla fall inte önskvärt, att utföra intervjuer eller genomföra studiebesök fysiskt. Istället har intervjuerna genomförts via telefon eller videosamtal, vilket har fungerat, men inte varit optimalt. Delvis beror detta på att ämnen som diskuteras begränsas till öppen information, vilket varit det förväntade resultatet för studien, men som kan ha påverkat respondenternas vilja att diskutera vissa områden. Det kan således gjort att svaren blivit mer restriktiva. Även avsaknaden av möjligheten till att se och läsa av individers kroppsspråk och icke-verbal kommunikation kan ha reducerat den erhållna informationsmängden.

Tidigt i studiens process identifierades räddningstjänsten som en värdefull informationskälla i rollen som innehavare och brukare av tunga fordon av vikt för civilförsvaret. Detta påverkade även i sin tur valet av respondenter starkt och resulterade i att fyra av fem intervjuer genomfördes med representanter från olika räddningstjänster i landet. Resultatet av dessa intervjuer har varit synnerligen värdefullt ur studiens synpunkt, men det hade även funnits ett värde och ett behov av att bredda urvalet även till andra verksamhetsområden som involverar tunga fordon. Exempelvis hade det varit önskvärt att kunna inkludera respondenter från transportsektorn samt från tredjeparts- eller påbyggnadsleverantörer i Sverige. Den främsta anledningen till att detta inte kunde genomföras inom ramen för studien var, utöver situationen med covid-19, brist på tid som indirekt uppstod på grund av ökad administration relaterad till lokala covid-19-regler.

7.2 Intervjuer och litteraturstudie

Resultatet för intervjufrågorna som berör studiens första frågeställning visar potentiellt hur arbetsroll och organisation kan påverka perspektiv. För samtliga respondenter från räddningstjänsten uppgavs att fysisk direktkontakt till fordon är den mest utsatta kommunikationskanalen. Studiens resterande respondent, tidigare benämnd som tillverkarrespondenten, delar dock bara delvis denna synpunkt då det även uppgavs att det finns hot för andra kommunikationskanaler där DoS-angrepp ses som det största hotet. Denna angreppstyp kan primärt sägas tillhöra kommunikationskanalen distans eller avstånd även om det kan utföras via alla kommunikationskanaler.

Kommunikationskanalen fysisk direktkontakt har varit en diskussionspunkt relaterat till tidigare studier, vilka har kritiserats eftersom de angrepp som påvisas i dessa studier har krävt fysisk tillgång till fordonet (Checkoway 2011; Miller & Valasek 2015). Det primära argumentet för kritiken har varit att om en antagonist har fysisk tillgång till fordonet kan denne direkt utföra fysiskt sabotage på fordonet, snarare än mer osäkra digitala angrepp. Detta eftersom digitala angrepp i regel är mer komplicerade att utföra än fysiskt sabotage. Andra studier har även kritiserats för att de angreppsexempel som presenteras är invecklade och kompetenskrävande, där kostnaden för att utföra angreppet inte överstiger vad som kan uppnås genom det. Det finns dock ett argument för att fysisk tillgång kan vara relevant för att utföra och dölja digitala angrepp som vid ett senare tillfälle får fysiska konsekvenser. Ett exempel kan vara att få en olycka att se ut att bero på ett mekaniskt fel snarare än ett digitalt angrepp, vilket är svårare att dölja i nätverkskommunikation på distans.

Av intervjuernas resultat att döma verkar det generellt som att mycket förtroende åläggs leverantörerna att korrekt hantera anslutningsmöjligheter i och med att ingen respondent uppgett att de granskar leverantörer ur cybersäkerhetssynpunkt. Däremot påpekar flera respondenter att anslutningstillfällen för leverantörer i service- eller uppdateringssyfte noga kontrolleras. Exempelvis i form av ansvarig hos respondentens organisation manuellt tillåter att en anslutning upprättas. Däremot är det inte helt tydligt om detta är till för att skydda fordon och system ur cybersäkerhetssynpunkt eller om det snarare handlar om att leverantörer inte omedvetet ska utföra service och uppdateringar när fordonen är i bruk eller har beredskap. Oavsett får detta positiva effekter cybersäkerhetsmässigt.

Många tredjeparts- eller påbyggnadssystem ansluts till de interna kommunikationsbussarna. Samtidigt har en del av dessa även anslutningsmöjlighet mot publika nätverk, vilket potentiellt kan utnyttjas av en angripare, liknande det som beskrivs i avsnitt 3.3. Från tillverkarens sida är det därför viktigt att begränsa vilka data som kan hämtas ut från de interna kommunikationsbussarna, samt vilka kommandon som kan skickas från påbyggnadssystem. I en del fall måste påbyggnadssystem kunna skicka kommandon för att styra interna ECU:er.

Exempelvis kan det vara nödvändigt för ett påbyggnadssystem att styra motor-relaterade ECU:er i syfte att förse systemet med tillräckligt med kraft för att utföra sin funktion.

Fordonstillverkare implementerar i regel ett påbyggnadsgränssnitt i sina fordon i syfte att ge tillgång och samtidigt begränsa instruktionsrättigheterna för tredje-parts- och påbyggnadsystem. Via gränssnittet kontrolleras vilka rättigheter alla anslutningar har i en form av vitlistning. Denna funktion går dock att kringgå då det via fysisk tillgång finns möjlighet att konfigurera om gränssnittet och sätta en godtycklig vitlistning av objekt.

Ingen av respondenterna uppger att man utvärderar sina leverantörer ur cyber-säkerhetssynpunkt i relation till inköp av fordon. Däremot uppgav flera respondenter att det är kommunen som ansvarar för inköp av andra system. Dessa inkluderar system och enheter vilka används inom fordonen, men som inte erbjuds av påbyggnadsleverantören. Exempelvis gäller detta för de bärbara datorer som används i räddningstjänstens fordon. Det är oklart hur beställnings-processen för dessa typer av produkter ser ut hos respektive kommun och om cybersäkerhet utvärderas i processen. Vidare skiljer sig eventuellt beställnings-processen åt mellan kommuner. Detta har inte utretts i studien då inga kommunala representanter intervjuats.

Från tillverkarens sida uppgavs att de har ett nära förhållande till sina olika leverantörer i syfte att förenkla och säkra utveckling och tillverkning av fordon. Exempelvis genom att säkerställa kunskap kring vilken funktionalitet som faktiskt finns i leverantörens olika komponenter och enheter. En sådan proble-matik kan exemplifieras i enlighet med vad som beskrivs i avsnitt 3.4 där Miller och Valasek (2015) upptäckte att D-Bus-systemet i experimentfordonet var bundet till alla nätverksgränssnitt och därmed gick att kommunicera med från distans. Det ska dock sägas att det är oklart om detta var en vald konstruktions-lösning eller inte. Risken är dock att detta var medvetet eftersom D-Bus-systemet underlättar implementation av nya funktioner.

Cybersäkerhetskunskap i relation till fordonen verkar vara på en generellt låg nivå hos användare. Slutsatsen dras främst utifrån avsaknaden av utbildningar i ämnet, samt att fordonen inte kravställs med avseende på cybersäkerhet. Anledningen till detta kan mycket väl vara att cybersäkerhet i relation till fordon är en relativt ny aspekt att ta hänsyn till och som tidigare inte varit relevant. Detta kan förklara varför arbetet med att utbilda inom området i nuläget ligger efter. Däremot uppgav flera respondenter att de får utbildning inom generell informationssäkerhet, vilket primärt täcker IT-kontorssystem, men som även kan ge effekt inom andra områden, vilket exempelvis skulle kunna inkludera fordon. Dessutom kan en ytterligare anledning till detta vara att det ännu inte skett några kända storskaliga angrepp som riktats mot fordon, eftersom negativ publicitet tenderar att påskynda säkerhetsarbete och utbildning. Kennedy, Holt och Cheng (2019) spekulerar i om den höga kunskapströskel som krävs för att angripa

fordon via cyberangrepp kan vara en anledning till att det ännu inte skett några (kända) angrepp mot fordon.

Det är värt att notera att tillgång till kommunikationsbussen som utomstående inte automatiskt innebär ett framgångsrikt angrepp. Detta beror på att person-säkerhetsfokuset i design och implementation motverkar extremhändelser. Exempelvis visade Miller och Valasek (2013) att autobromssystemet inaktiverades i händelse av motsägande kommunikation i just det fordon som de studerade. Alltså betyder detta att fordon för närvarande har ett visst inneboende skydd mot allvarliga fysiska konsekvenser av angrepp. Samtidigt innebär den alltmer omfattande implementationen av teknik i fordon att cybersäkerhets-riskerna ökar och därmed behöver cybersäkerhetsarbetet också öka.

8 Slutsats

Denna studie har ämnat undersöka sårbarheter hos tunga fordon av betydelse för civilförsvaret. Studiens fyra huvudfrågeställningar har alla, till viss del, kunnat besvaras.

Resultatet visar att cybersäkerhetsarbetet är mycket eftersatt, särskilt inom den tunga fordonsindustrin. Samtidigt ger för närvarande arbetet kring person-säkerhet ett visst skydd mot allvarligare händelser vid potentiella angrepp. Cybersäkerhetsarbetet behöver dock intensifieras inom en snar framtid i syfte att hålla jämna steg med den ökande datoriseringen av fordons kommunikations-arkitektur.

Fordonstillverkningsindustrin är dock medveten om problematiken kring cyber-säkerhet och utvecklar sitt arbete inom området. För närvarande ses DoS-angrepp som det potentiellt allvarligaste hotet mot tunga fordon. För samhällsviktig verksamhet skulle det vara förödande om fordonen inte gick att framföra.

Mängden forskning avseende cybersäkerhet i fordon, i synnerhet tunga fordon, är ytterst begränsad. Ett tecken på det är det låga antalet vetenskapliga artiklar inom området. Även respondenternas svar under intervjuerna visar på det. Dessutom utförs en majoritet av forskning idag på det amerikanska marknadssegmentet, vilket på sina håll skiljer sig från det europeiska. Det är därför viktigt att forskningen om cybersäkerhet i tunga fordon ökar inom EU och övriga Europa.

Det skulle även vara relevant för FOI att genomföra en fördjupande studie om teknisk cybersäkerhet i tunga fordon i syfte att ytterligare öka kunskapen inom området. Det skulle även vara av värde att utföra liknande intervjuer som i denna studie med en bredare repertoar av roller inom den tunga fordonsfären i enlighet med vad som beskrivs i avsnitt 7.1. En del av de tunga fordon som färdas på svenska vägar är av märken som inte är så vanliga i Sverige och har sin bas i andra länder. Därför kan det även vara relevant att se om det finns skillnader mellan länder i Europa gällande exempelvis lagstiftning som inte täcks av EU. Det kan även handla om skillnader vad gäller nyttjandet och implementationen av diverse system, däribland telematiksystem från tredje part.

Referenser

Argus Cybersecurity (2020). *A remote attack on an aftermarket telematics service*. https://argus-sec.com/remote-attack-aftermarket-telematics-service/ [2020-08-24].

Bluetooth Special Interest Group (SIG) (u.å.) *Understanding Bluetooth Range. https://www.bluetooth.com/learn-about-bluetooth/bluetooth-technology/range/* [2020-09-03].

Burakova, Y., Hass, B., Millar, L. & Weimerskirch, A. (2016). Truck hacking: An experimental analysis of the SAE J1939 standard. I *WOOT10, 10:e USENIX - Workshop on Offensive Technologies. Austin (Tx), USA 8–9 augusti 2016*. https://www.usenix.org/system/files/conference/woot16/woot16-paper-burakova.pdf

Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Schacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F. & Kohno, T. (2011). Comprehensive experimental analyses of automotive attack surfaces. I *20th USENIX Security Symposium. San Francisco (Ca), USA 8–12 augusti 2011, ss.77–92.* https://static.usenix.org/event/sec11/tech/full_papers/sec11_proceedings.pdf

Denscombe, M. (2014). *The good research guide: for small-scale social research projects.* McGraw-Hill Education (UK).

European Tyre & Rubber Manufacturers' Association (ETRMA) (2019). *Press Release: European General Road Safety Regulation Tyre Pressure Monitoring System – TPMS*. https://www.etrma.org/wp-content/uploads/2019/09/20190402-press-release-gsr-tpms-final.pdf

FMS-Standard (2004). *Ivan Hodac. Secretary General. Subject: CAN bus connection.* http://fms-standard.com/Truck/down_load/letter_acea.pdf

Garcia, F. D., Oswald, D., Kasper, T. & Pavlidès, P. (2016). Lock It and Still Lose It – On the (In)Security of Automotive Remote Keyless Entry Systems. I *Proceedings of the 25th USENIX Security Symposium. Austin (Tx), USA 10–12 augusti 2016, ss.929–944.* https://www.usenix.org/sites/default/files/sec16_full_proceedings.pdf

Gustafsson, T. & Valassi, C. (2018). *NCS3 – Kartläggning av elektroniska styrsystem i tunga fordon* (FOI Memo 6358). Stockholm: Totalförsvarets forskningsinstitut

Informationisbeautiful (2015). *Codebases: Millions of lines of code*. https://www.informationisbeautiful.net/visualizations/million-lines-of-code/ [2020-08-24].

ISO 11898-1:2015 *Road vehicles – Controller area network (CAN) – Part 1: Data link layer and physical signaling.*

ISO 15031-7. (2010). *Road Vehicles – Communication between vehicle and external equipment for emissions-related diagnostics – Part 7: Data link security*. utg. 2 https://www.iso.org/obp/ui/#iso:std:iso:15031:-1:ed-2:v1:en [2020-08-31].

Johansson K.H., Törngren M. & Nielsen L. (2005). Vehicle Applications of Controller Area Network. I Hristu-Varsakelis D. & Levine W.S. (red.) *Handbook of Networked and Embedded Control Systems*, ss.779–792. Boston: Birkhäuser Boston. https://doi.org/10.1007/0-8176-4404-0_32

Jonson, U. (2018). *Heavy Vehicle Cybersecurity Program* [presentation]. Auto-ISAC Monthly Community Call, 4 april. https://www.automotiveisac.com/wp-content/uploads/2018/05/03_29_18_Auto-ISAC-April-4-Community-Call-_FINAL.pdf

Kennedy, J., Holt, T. & Cheng, B. (2019). Automative cybersecurity: accessing a new platform for cybercrime and malicious hacking. I *Journal of Crime and Justice*, 42(5), ss.632–645. DOI: https://doi.org/10.1080/0735648X.2019.1692425

Metzger, M. (2010). Letting the air out of Tire Pressure Monitoring Systems [video]. *DEFCON 18*. Las Vegas (Nv), USA 30 juli–1 augusti 2010. https://www.youtube.com/watch?v=gUsE9aTLYnk [2020-11-24]

Miller, C. & Valasek, C. (2013). Adventures in automotive networks and control units [video]. *Def Con 21*..Las Vegas (Nv), USA 1–4 augusti 2013. https://www.youtube.com/watch?v=n70hIu9lcYo [2020-11-25]

Miller, C. & Valasek, C. (2015). Remote exploitation of an unaltered passenger vehicle [video]. *Black Hat 15*. Las Vegas (Nv), USA 1–6 augusti 20915. https://www.youtube.com/watch?v=MAcHkASmXEc [2020-11-25]

Mukherjee, S., Van Etten, J. C., Samyukta, N. R., Walker, J., Ray, I. & Ray, I. (2019). TruckSTM: Runtime Realization of Operational State Transitions for Medium and Heavy Duty Vehicles. *ACM Transitions on Cyber-Physical Systems*, 4(1), ss.4–25. DOI: https://doi.org/10.1145/3300183

Norte, J., K. (2016). Hacking industrial vehicles from the internet [blog]. *Jose Carlos Norte Personal Blog*, 6 mars. http://jcarlosnorte.com/security/2016/03/06/hacking-tachographs-from-the-internets.html [2020-11-25]

Pazul, K. (1999). *Controller area network (CAN) basics* (AN713). http://ww1.microchip.com/downloads/en/AppNotes/00713a.pdf

Richards, P. (2002). *A CAN physical layer discussion* (AN228). http://ww1.microchip.com/downloads/en/appnotes/00228a.pdf

SAE J1979. (2017). *E/E Diagnostic test modes J1979_201702*. https://www.sae.org/standards/content/j1979_201702/ [2020-08-31]

Scania (2017). *Användning och ansvar*. *https://bodybuilder.scania.com/trucks/sv/about-tbb/use-and-responsibility.html* [2020-09-03].

Stachowski, S., Bielawski, R. & Weimerskirch, A. (2018). *Cybersecurity Research Considerations for Heavy Vehicles* (DOT HS 812 636). Washington, DC: National Highway Traffic Safety Administration (NHTSA). https://deepblue.lib.umich.edu/bitstream/handle/2027.42/151379/UMTRI-2018-10.pdf

Strobel, O. (red.). (2013). *Communication in transportation systems*. IGI Global.

SFS 2001:559. *Lag (2001:559) om vägtrafikdefinitioner.* Stockholm: Infrastrukturdepartementet.

Tollefson, R. (2019). As the connectivity of trucking fleets grows, so do cybersecurity risks. *Infosec*, 10 april. https://resources.infosecinstitute.com/topic/as-the-connectivity-of-trucking-fleets-grows-so-do-cybersecurity-risks/ [2020-11-05]

Trafikanalys (2019a). *Lastbilstrafik 2019*. https://www.trafa.se/globalassets/statistik/vagtrafik/lastbilstrafik/2019/lastbilstrafik-2019.pdf

Trafikanalys (2019b). *Järnvägstransporter 2019 kvartal 4*. https://www.trafa.se/globalassets/statistik/bantrafik/jarnvagstransporter/2019/jarnvagstransporter-2019-kvartal-4.pdf

Transportstyrelsen (2015). *Personbil*. https://www.transportstyrelsen.se/sv/vagtrafik/Fordon/Fordonsregler/Personbil/ [2020-04-03].

Weimerskirch, A., Becker, S. & Hass, B. (2017). Commercial Vehicle vs. Automotive Cybersecurity – Commonalities & Differences. I D'Anna, G. *Cybersecurity for Commercial Vehicles*. SAE International. http://www.weimerskirch.org/files/WeimerskirchBeckerHass_CommercialVehicleVsAutomotiveCybersecurity.pdf [2020-11-10].

Winning, A. (2019) Number of automotive ECUs continue to rise. *eeNews automotive*, 15 maj. https://www.eenewsautomotive.com/news/number-automotive-ecus-continues-rise [2020-08-24].

Bilaga A: Intervjuguide

Denna studie utförs av Totalförsvarets forskningsinstitut på uppdrag av Myndigheten för samhällsskydd och beredskap.

Studiens mål är att undersöka sårbarheter hos tunga fordon av betydelse för civilförsvaret. För att uppfylla detta mål ska studien besvara följande huvudfrågor:

- Vilken kommunikationskanal medför den största risken för att ett fordon otillbörligen kan påverkas (vid direktkontakt närhet eller på avstånd)?
- Vilka cybersäkerhetsrisker innebär tredjepartssystem/ombyggnationer av fordon?
    - Vilka konsekvenser kan dessa risker få?
- Hur utvärderar beställare sina specialleverantörer (karosseri och ombyggnad) ur en cybersäkerhetssynvinkel?
- Vilken kunskap har berörda intressenter gällande cybersäkerhet i tunga fordon?

Dessa frågor har använts som grund för skapandet av denna intervjuguide, där varför fråga utgör en kategori med flera relaterade underfrågor. Nedan listas intervjuguidens alla frågor i sin helhet.

Introduktion
Notera att respondenten själv får välja vilken av denna personliga information som inkluderas i studien.

Respondentens namn:

Titel:

Organisation:

Bakgrund:

Annan relevant information:

Finns det en uttalad process hos er för att hantera cybersäkerhetsfrågor relaterat till tunga fordon?

- **Hur ser den ut?**
- **Brister?**
- **Fördelar?**

Hur ser beställningsprocessen ut för tunga fordon ut?

- **Finns det samarbeten med andra regioner?**
- **Finns det nationella riktlinjer?**

- **Avtal/upphandling**
- **Specifika leverantörer?**
- **Hur ser det ut på nationell nivå?**
- **Finns det skillnader mellan beställningsprocessen för tunga fordon och andra specialfordon (ex. polisfordon eller ambulans)?**
- **Finns det cyberfysisk funktionalitet som inte alltid nyttjas i de karosserier ni bygger?**
- **Vilka möjligheter finns det för beställare att skräddarsy system/produkter i de fordon ni tillverkar? (installeras saker de inte vet hur de fungerar?)**
- **Informerar/utbildar ni (karosseri) kunder/mottagare gällande cybersäkerhetshot mot systemen ni levererar? (korrekt användning, nytta av uppdatering osv.)**
- **Granskar ni de system ni installerar ur ett cybersäkerhetshots perspektiv?**

Vilka cybersäkerhetskrav ställer ni som beställare på leverantörer av tunga fordon?

Hur ser ni på kravställning och användning av ny teknik i de produkter ni beställer?

- **Ex. over-the-air uppdateringar?**

Hur används de produkter/fordon ni beställer?

- **Lämnas fordon obevakade/olåsta när de är ute på uppdrag?**
- **Hur används tekniken i fordonen?**
- **Gör ni egna justeringar/implementationer av teknik/produkter i fordonen? (ex. mjukvara i form av FMS)**
- **Hur sköts underhållet av fordonens cybertekniska system?**
- **Hur sköts underhållet av fordonens mekaniska system?**
- **Hur lång är livslängden på en produkt (ex. en brandbil)?**
- **Görs det större ombyggnationer/uppgraderingar för att förlänga livslängden och införa nya system?**
- **Hur meddelas användare om ny funktionalitet efter uppdatering?**

Vilken kommunikationskanal medför den största risken för att ett fordon otillbörligen kan påverkas (vid direktkontakt, närhet eller på avstånd)?

- **Finns det anslutningar till den interna kommunikationsbussen som kan nås från utsidan av fordonet?**

Vilka cybersäkerhetsrisker innebär tredjepartssystem/ombyggnationer av fordon?

- **Vilka konsekvenser kan dessa risker få?**

Hur utvärderar beställare sina specialleverantörer (karosseri och ombyggnad) ur en cybersäkerhetsvinkel?

Vilken kunskap har berörda intressenter gällande cybersäkerhet i tunga fordon?

Hur hanteras over-the-air-uppdateringar (OTA)? Mjukvarunycklar osv.

- **Hur verifieras att uppdateringar har gjorts och att genomförandet var korrekt?**
- **Hur hanteras ofullständigt genomförda uppdateringar?**
- **Hur vet man som brukare att fordonets system har uppdaterats?**
- **Hur meddelas användare om ny funktionalitet efter uppdatering?**
- **Hur påverkas fordonets framfart av OTA?**

Bilaga B: Intervjuförfrågan

Hej [Namn]!

Jag heter Martin Karresand och är forskare samt projektledare på Totalförsvarets forskningsinstitut (FOI). Just nu genomför jag och min kollega Christian Valassi en studie angående cyberfysiska sårbarheter i tunga fordon. Inom denna studie skulle vi gärna vilja intervjua dig med frågor om exempelvis cybersäkerhet i tunga fordon generellt, cybersäkerhet relaterat till tredjepartssystem samt hot och risker. Vi har en relativt bred forskningsansats och söker individer som kan belysa våra frågeställningar från olika perspektiv. Vi är därmed också medvetna om att alla respondenter inte kommer kunna svara på alla frågor.

Skulle du vilja ställa upp på en sådan intervju?

Intervjun kan i första hand genomföras via telefon då rådande situation med covid-19 begränsar möjligheter att ses i person. Vi utesluter dock inte ett möte i person om så är önskvärt från eran sida, där det exempelvis är tänkbart att genomföra intervjun utomhus.

Projektet utförs på uppdrag av Myndigheten för samhällsskydd och beredskap (MSB) under samarbetet NCS3 (www.foi.se/ncs3). Kontaktperson på MSB för detta projekt är Gustav Söderlind.

Syftet med studien fås ur uppdragstexten:

FOI genomförde 2017 en studie om tunga fordon. Syftet med den studien var att översiktligt kartlägga system och teknologier som används i tunga fordon. Denna studie bygger vidare på det tidigare arbetet från 2017 genom att undersöka vilka sårbarheter som etablerade teknologier och system i tunga fordon kan medföra.

Studien ska besvara följande övergripande frågeställningar:

- Vilken kommunikationskanal medför den största risken för att ett fordon otillbörligen kan påverkas (vid direktkontakt, närhet eller på avstånd)?
- Vilka cybersäkerhetsrisker innebär tredjepartssystem/ombyggnationer av fordon?
    - Vilka konsekvenser kan dessa risker få?
- Hur utvärderar beställare sina specialleverantörer (karosseri och ombyggnad) ur en cybersäkerhetssynvinkel?
- Vilken kunskap har berörda intressenter gällande cybersäkerhet i tunga fordon?

Om ni vill ha tillgång till alla intervjufrågor kan dessa skickas på förhand.

Avslutningsvis ska sägas att studien kan komma att omfattas av sekretess, beroende på vilken information som samlas in under studien. Det bör dock

tilläggas att vi inte är ute efter information gällande sårbarheter eller angrepp relaterat till specifika fordonstillverkare eller modeller.

Har du några frågor eller funderingar är du välkommen att kontakta mig eller min kollega Christian.

Tack på förhand!

FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
164 90 Stockholm

Tel: 08-55 50 30 00
Fax: 08-55 50 31 00

www.foi.se