NCS3 – Elektroniska styrsystem i tunga fordon

Projektnummer/Project no

E72268

Kund/Customer

MSB

FoT-område

Handläggare/Our reference

Tommy Gustafsson

Datum/Date

2018-03-01

Memo nummer/number

FOI Memo 6358

NCS3 - Kartläggning av elektroniska styrsystem i tunga fordon

Innehållsförteckning

1 Inledning

Detta memo är resultatet av en studie som *Myndigheten för Samhällsskydd och Beredskap* (MSB) har beställt inom ramen för *Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet* (NCS3). I detta memo presenteras en översiktlig kartläggning över system och teknologier som används i tunga fordon med fokus på:

- hur dessa är sammankopplade
- hur de kopplar upp sig på nätet
- vilka delar som pratar med vilka

Med tunga fordon avses lastbilar (bil som är inrättad huvudsakligen för godstransport) och bussar (bil som är byggd huvudsakligen för persontransporter och är försedd med fler än åtta sittplatser utöver förarplatsen) (Transportstyrelsen u.å.)

Utvecklingen inom smarta fordon (uppkopplade, kommunicerande, självkörande) sker snabbt både inom förarassisterande system och inom autonoma fordon. Ett annat exempel på detta är att Sveriges regering under 2017 fastslog en förordning för försöksverksamhet med självkörande fordon (SFS 2017:309). Samtidigt har flera forskningsrapporter påvisat brister i cybersäkerheten hos de teknologier som används inom fordonsindustrin, vilket väcker många nya frågor. Flera av dessa studier har dock genomförts på personbilar och bilden över huruvida de brister som påvisats även föreligger hos tunga fordon är därför något oklar. Syftet med detta memo är att ta fram ett underlag med fokus på elektroniska styrsystem i tunga fordon. Underlaget ska användas för att bedöma cybersäkerhetsrelaterade konsekvenser av denna utveckling samt att kunna bedöma behovet av framtida cybersäkerhetsanalyser.

I memot presenteras system och teknologier som används idag och som bedöms användas på fem–tio års sikt.

1.1 Genomförande

Studien har i huvudsak genomförts genom internetsökningar på relevanta termer. De teknologier och system som är relevanta för området har successivt identifieras och presenteras i detta memo. Studien har också inkluderat en intervju med en tillverkare av tunga fordon samt samtal med ett företag som bedriver kollektivtrafik och som är användare av tunga fordon. Den insamlade informationen från internetsökningar och intervjuer har sedan analyserats och sammanställts i text och grafik.

1.2 Avgränsning

Studien omfattade endast den teknologi som används i tunga fordon och inkluderar inte personbilar, motorredskap eller anläggningsmaskiner. Studien uppgift har heller inte varit att analysera eventuella risker eller hot relaterade till de aktuella systemen. Vidare skulle studien endast beskriva teknologierna på en överskådlig nivå utan att gå in på enskilda fordon eller tillverkare.

Tidshorisonten för studien har begränsats till att beskriva de system som används för närvarande och som kan vara aktuella på fem till tio års sikt. Av denna anledning ingår endast begränsade studier av autonoma fordon och teknologier i studien.

1.3 Läshänvisning

I detta memo beskrivs olika system i tunga fordon som utnyttjar intern och extern kommunikation för att ge läsaren en allmän förståelse för behovet av kommunikation. Därefter beskrivs övergripande uppbyggnad av den interna kommunikationen samt ingående komponenter under rubriken Systemkomponenter. Under rubriken Kommunikation beskrivs olika nätverksprotokoll och deras övergripande användning. Memot

avslutas med ett diskussionsavsnitt som värderar studiens resultat och vilka lärdomar som detta ger med avseende på cybersäkerhet relaterad till tunga fordon.

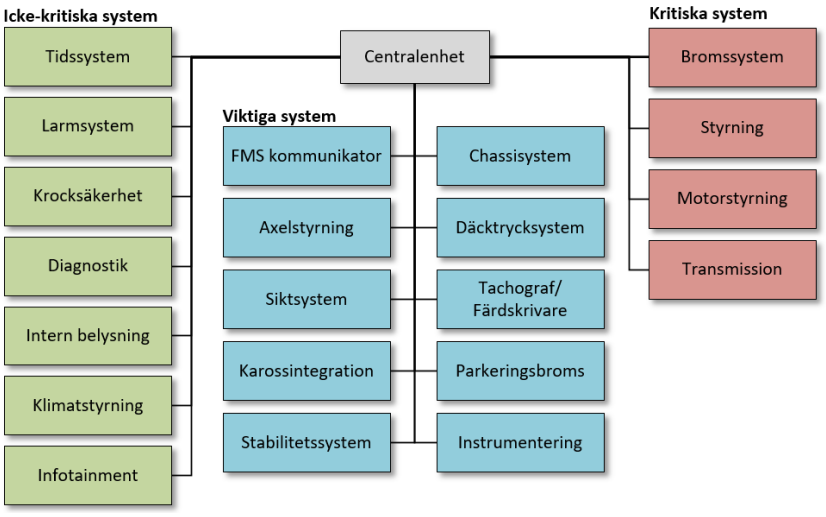
2 System

Ett modernt fordon har ett stort antal elektroniska styrsystem som interagerar och kommunicerar med varandra och med omvärlden. Den interna kommunikationen sker i hög grad med olika nätverksprotokoll som i första hand har utvecklats för att vara robusta men som saknar funktioner för cybersäkerhet. Det stora antalet system och deras interaktion inom och utanför fordonet medför att fordon idag är mer känsliga för cyberangrepp. Under denna rubrik beskrivs exempel på system samt hur de interagerar med varandra.

Ett sätt att kategorisera systemen är att se till systemens funktion och påverkan på fordonets framförande. En första grupp utgörs av fordonstekniska system som motorstyrning, avgasrening och bromsar. En andra grupp utgörs av interna säkerhetssystem som till exempel kontrollerar elektroniska nycklar, att säkerhetsbältet används samt att dörrar är stängda. Ur ett cybersäkerhetsperspektiv är den senare gruppen inte så känslig eftersom de egentligen inte påverkar fordonets framförande. Möjligtvis kan en attack mot dessa system leda till att fordonet stannar.

Som en följd av de elektroniska styrsystemen har utvecklingen av system som på olika sätt assisterar föraren och som påverkar framförandet av fordonet ökat och idag sker omfattande utveckling mot allt mer autonoma fordon. Samtidigt har utvecklingen av samverkan med system utanför fordonet ökat, till exempel med IT-system som tillåter fordonets ägare och tillverkare att kontrollera fordonets status eller utbyta information med system i andra fordon i närområdet. I båda dessa fall ökar risken kopplad till cyberangrepp eftersom de dels påverkar fordonets framförande och dels exponerar interna system för omvärlden.

Även fordonstillverkarna delar generellt in systemen i olika kategorier baserat på hur kritiska de är för fordonets framförande och det förefaller vanligt att man också helt eller delvis segmenterar kommunikationsbussen[1] i enlighet med denna indelning (Axelsson et al., 2003; Johansson et al., 2005; Scania Truck Bodybuilder, 2016). I detta memo delas systemen fortsättningsvis in i kategorierna *Kritiska*, *Viktiga* och *Icke-kritiska*. Figur 1 baseras på samma källor och visar ett antal exempel på system i moderna tunga fordon samt en generalisering över hur fordonstillverkarna delar in dessa. Antalet system, deras benämningar och uppbyggnad samt graden av integration eller isolering varierar mellan fordonstillverkare, fordonsgenerationer och tillverkningsår.



Figur 1: Kategorisering av elektroniska styrsystem i tunga fordon baserat på nivån av inflytande systemet har på fordonets funktion. Begränsad kommunikation mellan dessa system tillåts ofta via en centralenhet (Axelsson et al., 2003; Johansson et al., 2005; Scania Truck Bodybuilder, 2016).

[1] 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 innehåller flera kommunikationsbussar som är segmenterade och som ibland använder olika nätverksprotokoll.

Kommunikation mellan systemen är ofta segmenterad genom en centralenhet. Centralenheten i mitten är en specialiserad styrenhet som begränsar kommunikationen mellan de olika systemen men vissa insignaler och funktioner kan passera centralenheten[2]. Tills nyligen har denna segmentering enligt samma källa baserats på behovet av robusta system snarare än på cybersäkerhetsaspekter. Detta tankesätt från fordonsindustrin kan vara en anledning till att flera forskargrupper har kunnat attackera kritiska system i personbilar genom att gå via icke-kritiska system (Miller & Valasek, 2015; Checkoway et al., 2011). Nedan följer en beskrivning av respektive kategori samt exempel på system som tillhör respektive kategori. Dessutom ges tre exempel på övergripande system där olika system i tunga fordon samverkar.

2.1 Kritiska System

Kritiska system är de system som direkt påverkar fordonets framförande. Ett rimligt antagande är att ju högre grad av autonomi som fordonet har, desto viktigare blir det att skydda dessa system mot cyberangrepp. Exempel på kritiska system är bromssystem, system som kan styra fordonet och system som påverkar motor och växellåda vilka i sin tur kan påverka fordonets hastighet (Scania Truck Bodybuilder, 2016).

2.2 Viktiga System

Med *Viktiga system* menas system som är viktiga för fordonets framförande men som inte kan påverka säkerhetskritiska funktioner. Dessa system inkluderar tekniska system såsom instrumentering, stabilitets- och axelstyrning samt belysning och siktsystem. Viktiga system inkluderar också administrativa system såsom färdskrivare och kommunikation med centrala IT-system samt integrationsgränssnitt för tredjepartssystem via karossintegrationer (Scania Truck Bodybuilder, 2016).

2.3 Icke-kritiska system

Benämningen *Icke-kritiska system* innefattar de system som varken är kritiska eller viktiga för fordonets framförande eller säkerhet. I denna kategori ingår de system som till största andel ger ökad komfort och funktionalitet för föraren. Exempel på system är infotainment, innerbelysning, klimatstyrning och larmsystem. Ett par intressanta system ur ett cybersäkerhetsperspektiv i denna kategori är diagnostikuttag och tidssystem då dessa verkar kunna kommunicera med, och påverka, andra viktigare system (Scania Truck Bodybuilder, 2016).

2.4 Fleet Management System

Fleet Management System (förkortas allmänt FMS) är ett system som låter fordonets operatör planera och optimera nyttjandet av fordon och förare. FMS är ett exempel på ett externt IT-system som samlar in information från fordonet såsom status, bränslekonsumtion, bränslenivåer, position och körtider. I många FMS-system finns det också möjlighet att skicka meddelanden till fordonet som föraren kan ta del av i sina uppdrag ute på vägarna.

FMS-system är av ekonomiska skäl särskilt viktiga för tunga fordon eftersom ett optimalt nyttjande av fordonet är direkt kopplat till lönsamheten. Hur viktigt FMS är för hanteringen av tunga fordon exemplifieras av att det finns en öppen standard för FMS som utvecklades av de europeiska fordonstillverkarna MAN AG, Scania, Volvo Trucks, DAF Trucks, Daimler AG och IVECO år 2002 (FMS-Standard 2004). Ett av målen med denna standard var att ge tillgång till fordonsinformation åt fordonets ägare utan att riskera osäkra uppkopplingar in mot den interna kommunikationsbussen. Både Scania (Connected Services) och Volvo (Connected Truck) har utvecklat egna system som ska göra det enklare och kostnadseffektivare att hantera fordonet. Dessa system har också kopplingar till externa enheter

[2] Systemexpert, Scania, Telefonintervju 2017-12-15

såsom mobiltelefoner och smarta klockor där föraren kan utföra vissa funktioner samt få information om fordonets status. FMS-system är i detta sammanhang intressanta eftersom de kombinerar flera teknologier (såsom trådlös kommunikation och åtkomst till elektroniska styrsystem) som utgör möjliga angreppsvektorer för cyberangrepp mot tunga fordon.

2.5 Tredjepartssystem

Det finns en betydande tredjepartsutveckling av IT-system som interagerar med elektroniska styrsystem i tunga fordon. I första hand rör det sig om FMS framtagna av olika tjänsteleverantörer (Trakm8, 2018; Fleetboard, 2018). I vissa fall kopplas dessa system in direkt på fordonets interna kommunikationsbussar vilket riskerar att påverka fordonets elektroniska styrsystem på ett sätt som varken tredjepartsleverantören, tillverkaren eller ägaren avsett eller insett (Trakm8, 2011). Europeiska fordonstillverkare (däribland Volvo och Scania) tillåter inte denna typ av inkoppling direkt på kommunikationsbussen utan har i ett brev till EU beskrivit sådan inkoppling som extremt farlig och att en sådan inkoppling förverkar fordonets garanti (FMS-Standard, 2004). Då dessa tredjepartssystem som regel också innehåller någon form av extern kommunikationslänk (till exempel 3G/4G) så kan detta vara en möjlig vektor för cyberangrepp.

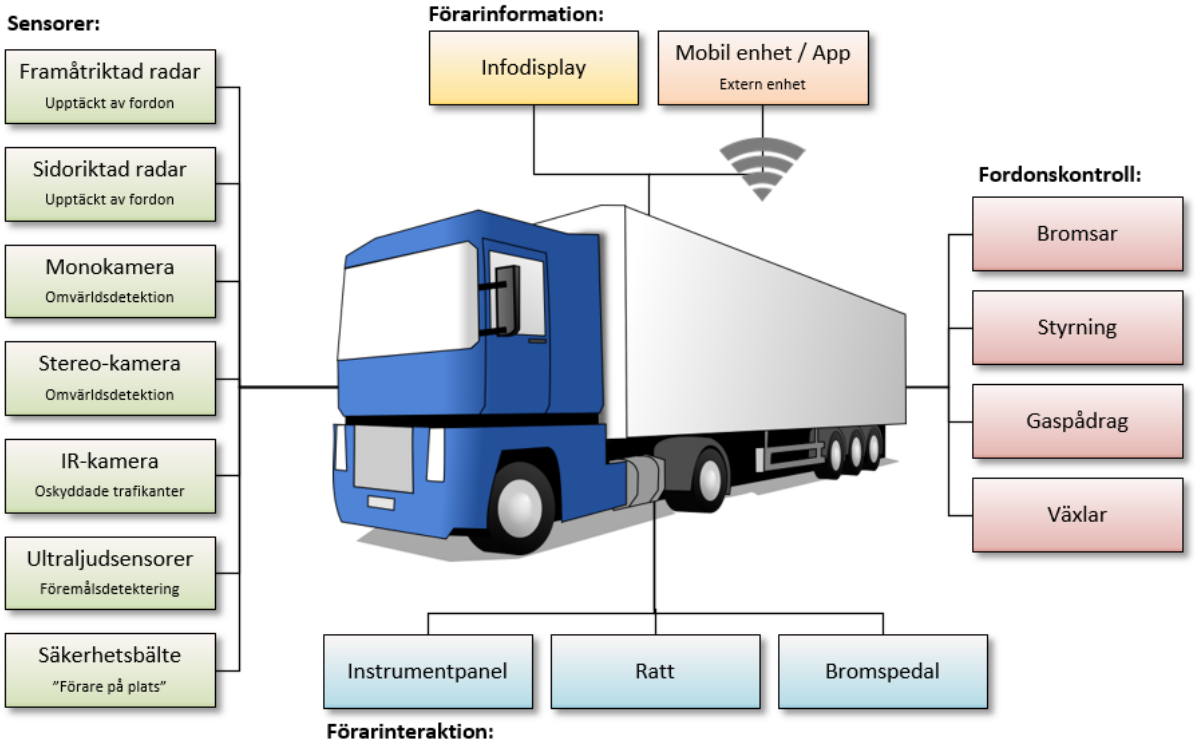
En annan typ av tredjepartssystem för tunga fordon är de system som utvecklas av ägaren eller operatören av fordonen. Exempel på sådana system finns inom kollektivtrafik där operatören vill förmedla fordonets position till resenären eller att ta betalt för resan[3]. Det förekommer att dessa system innehåller egna kommunikationslösningar och att de i vissa fall kopplas in på fordonets interna kommunikationsbuss.

2.6 Autonoma system

Självkörande eller autonoma tunga fordon utgör en utmaning ur ett cybersäkerhetsperspektiv då dessa system tillåter att fordonet framförs endast med hjälp av elektroniska signaler som skulle kunna påverkas via cyberangrepp. Om ett sådant system utvecklas utan att man tar hänsyn till cybersäkerhetsaspekter är det med andra ord tänkbart att en angripare eller ett systemfel direkt påverkar fordonets framförande.

Utvecklingen inom förarassisterande och autonoma system går fort och bygger i hög grad på samverkan mellan fordonets elektroniska styrsystem. För att beskriva hur långt utvecklingen hunnit i skrivandets stund samt för att ge en bild av hur dessa system interagerar med fordonets elektroniska styrsystem beskrivs under denna rubrik ett exempel på ett autonomt system. Systemet visas i Figur 2 och är baserat på försök som Scania och MAN har gjort med en så kallad Traffic Jam Pilot (nedan kallad autopilot) där systemet har förmågan att framföra fordonet autonomt i en långsamtgående bilkö (Chamoun, 2014).

[3] Systemexpert, Östgötatrafiken, Telefonintervju 2017-12-19



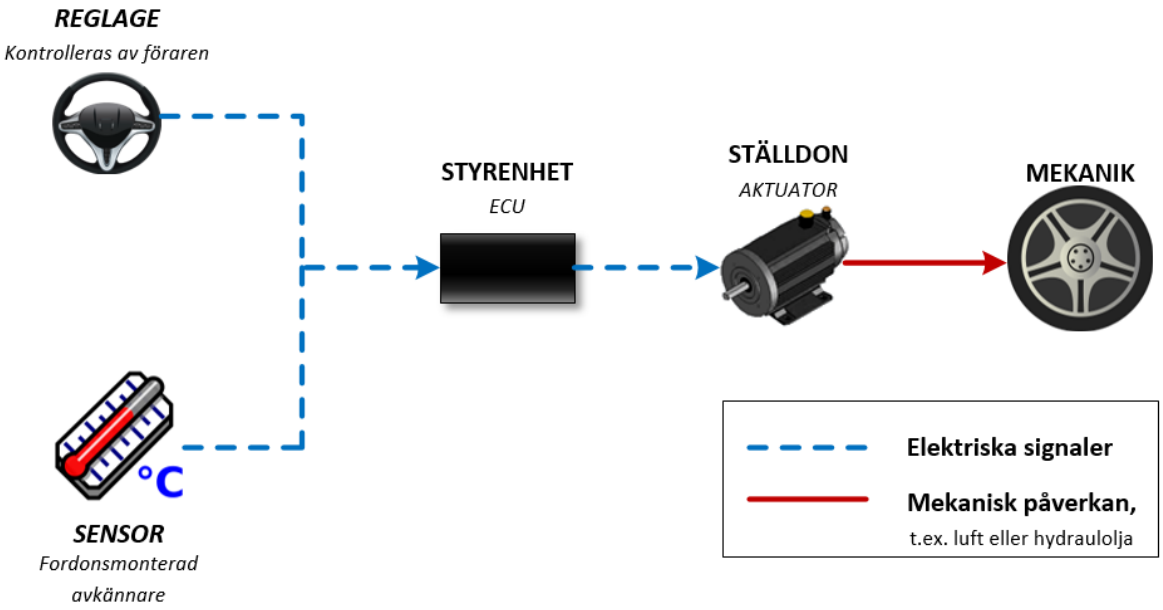
Figur 2: Figuren visar exempel på hur system samverkar för att ett tungt fordon ska kunna framföras delvis autonomt.

Målet med autopiloten är att chaufförен kan ägna sig åt andra arbetsuppgifter eller kanske få sin viloperiod. Autopiloten bygger på att ett antal sensorer samlar in data om fordonets omgivning såsom vägens sträckning, omgivande trafik, föremål på vägbanan samt oskyddade trafikanter. Dessa data sammanställs och används sedan för att kontrollera fordonets styrning och hastighet. Chaufförен hålls hela tiden informerad via fordonets instrumentpanel och via en extern enhet i form av en läsplatta. Om en situation som systemet inte kan hantera skulle uppstå så kan till exempel nödbromsen aktiveras. Försöken genomfördes under 2014 och visar ett autonomt system som har liknande funktionalitet som den autopilot som Audi introducerar i modell A8 under 2018 (Audi Technology Portal, 2017).

3 Systemkomponenter

I detta kapitel presenteras ett antal komponenter för elektroniska styrsystem i moderna fordon. Figur 3 visar en förenklad skiss för hur ett elektroniskt styrsystem i ett fordon är uppbyggt.

Elektroniska styrsystem bygger på att ett reglage som kontrolleras av föraren eller en sensor genererar en insignal till en specialiserad styrenhet. Denna insignal bearbetas i styrenhetens programvara och leder i sin tur till att en styrsignal skickas till ett eller flera ställdon (ofta kallade aktuatorer efter engelskans actuators). Ställdonet påverkar sedan en fysisk komponent såsom bromsar eller styrning som i sin tur påverkar fordonets framförande. Styrsignalerna mellan systemkomponenterna skickas via elektroniska kommunikationsbussar, ofta refererad som CAN-buss. CAN är en förkortning för Controller Area Network men är endast ett av de nätverksprotokoll som används inom tunga fordon varför denna användning är en något felaktig generalisering. Se avsnittet 4 - *Kommunikation i fordon* för en utförlig genomgång av de nätverksprotokoll som används i tunga fordon.



Figur 3: Skissen visar principen för hur ett elektroniskt styrsystem är uppbyggt i ett fordon. En styrenhet mottar en insignal, genomför en beräkningsoperation och skickar en styrsignal som påverkar fordonet.

Principen i Figur 3 används idag på ett eller annat sätt för att kontrollera de flesta funktioner i ett fordon. Ofta samverkar dessa system. Utsignaler eller värden från en styrenhet kan läsas av andra styrenheter och fungerar då som styrdata till dessa. Ett exempel på ett sådant system i tunga fordon är ett system som mäter fordonets lutning och som använder denna information för att bromsa fordonet om hastigheten är för hög i en kurva[4]. Denna samverkan möjliggörs genom systemen delar kommunikationsbuss.

Värt att notera är att system och komponenter varierar mellan tillverkare, modell och tillverkningsår. Detta gör det svårt att få en överblick över exakt vilken påverkan ett cyberangrepp skulle få på ett visst fordon.

3.1 Drive-by-wire

Historiskt har elektronik används för att styra vissa funktioner i fordonen, till exempel bränsletillförsel till motorn, men i takt med utvecklingen av elektroniska styrsystem har allt mer funktionalitet överförts från rent mekaniska system till elektromekaniska system. Drive-by-wire (alternativt *x*-by-wire där ”*x*” ersätts av namnet på det system som avses till exempel ”*steer*” eller ”*brake*”) är en samlingsterm som används för

[4] Lastbilschaufför, Scania, Intervju 2017-12-12

system där endast elektroniska komponenter används för att kontrollera framförande av personbilar och tunga fordon (Dittmer, 2001).

Drive-by-wire innebär att det inte finns någon mekanisk koppling mellan det reglage som kontrolleras av föraren (till exempel ratten eller gaspedalen) och den mekaniska komponent som reglaget påverkar. Denna utveckling drivs av att mekaniska komponenter såsom rattstång, pumpar och hydraulik kan tas bort ur fordonen vilket minskar komplexiteten samtidigt som det spar utrymme och vikt. Det har också medfört att olika system som tidigare var svåra att koppla ihop numera kan interagera genom att en styrsignal skickas till flera styrenheter eller genom att resultatet från en styrenhet kan användas som indata till ett annat system.

Övergången till drive-by-wire har medfört att det är möjligt att framföra ett fordon med endast elektroniska styrsignaler vilket i sin tur möjliggjort en betydande utveckling av helt eller delvis autonoma fordon. Autonomi riskerar att öka betydelsen av cybersäkerhet i de elektroniska styrsystemen eftersom ett cyberangrepp kan få större påverkan på fordonet, till exempel genom att påverka styrning eller hastighet. Miller och Valasek (2015) har i sin forskning påvisat att en förare kan motverka effekten av ett angrepp genom att till exempel styra emot med ratten. En relevant frågeställning blir då hur snabbt en förare reagerar om man använder ett semi-autonomt system såsom det som beskrivs under avsnittet Autonoma system.

3.2 ECU

ECU (Electronic Control Unit) är en allmän förkortning som används för en styrenhet i ett fordon. Dessa styrenheter har likheter med industriella styrsystem inom andra branscher genom att det i huvudsak rör sig om robusta beräkningsenheter med specifika uppgifter, men som i hög grad nyttjar branschspecifika standarder och kommunikationsprotokoll. Det är vanligt att styrenheterna ges namn baserat på det system de ingår i, till exempel Brake Control Module eller Transmission Control Unit (BCM respektive TCU) (Scania Truck Bodybuilder, 2016). Namn, förkortningar och systemens funktion skiljer 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.

Antalet styrenheter som finns i tunga fordon varierar baserat på tillverkare, tillverkningsår, modell och fordonets funktioner. Resultatet av ett par sökningar på internet ger slutsatsen att det är rimligt att anta att det finns ett hundratal styrenheter i ett modernt fordon. Dessa sökningar indikerar också att antalet styrenheter växer samt att olika system i allt högre grad kommunicerar med varandra.

3.3 Mjukvara

Ett allmänt accepterat faktum är att antalet sårbarheter ökar med mängden mjukvara och moderna fordon innehåller en stor mängd mjukvara. En uppskattning gjord 2009 hävdar att antalet rader kod i en modern personbil närmar sig 100 miljoner (Charette, 2009). Baserat på mängden elektroniska styrsystem i tunga fordon och att det finns stora likheter mellan dessa och de system som finns i personbilar, är det rimligt att anta att även dessa innehåller stora mängder mjukvara.

Sökningar på Internet och samtal med ett företag som bedriver trafik med tunga fordon indikerar att mjukvaran i ett fordon inte kan ses som en sammanhållen mjukvara utan att det snarare är ett antal samverkande system där mjukvaran utvecklas av olika aktörer. I denna studie har det inte funnits möjlighet att genomföra någon djupare analys av mjukvaran i tunga fordon men nedan presenteras det övergripande sambandet mellan de aktörer som utvecklar mjukvaran för tunga fordon.

Fordonstillverkarna köper in fysiska komponenter från underleverantörer (Autoline, 2018). Det är oklart huruvida underleverantörerna själva utvecklar sin mjukvara eller om de i sin tur förlitar sig på egna underleverantörer. Fordonstillverkarna utvecklar sedan mjukvara som interagerar med mjukvaran i komponenterna samt system där in- och utdata från flera komponenter hanteras och påverkar fordonet. I

många fall kopplas elektroniska styrsystem i fordonet upp till IT-system utanför fordonet[5]. Både Volvo och Scania tillhandahåller som tidigare nämnts system där mjukvara i fordonet interagerar med IT-system utanför fordonet, så kallade Fleet Management System.

Utöver denna mjukvara förekommer det också en betydande utveckling av mjukvara hos tredje part. Det finns exempel på ett företag som använder tunga fordon och som utvecklar egna IT-system som interagerar med elektroniska styrsystem i fordonen. Sådana system kan till exempel låta resenärerna se positionen för en buss och låta företaget övervaka fordonens position och status[6]. En annan form av aktörer är rena tjänsteleverantörer som utvecklar IT-system som används av de som opererar tunga fordon, till exempel tillverkaroberoende FMS-system (Trakm8, 2018; Fleetboard, 2018).

3.4 Reglage

Reglage avser den komponent som fordonets förare eller passagerare använder för att påverka ett system i fordonet, alltifrån en ratt till knappar och elektroniska touchreglage.

En annan utveckling som framgår av sökningar på tillverkarnas hemsidor och på internet är att det har blivit vanligare att reglagen i sig innehåller enklare styrenheter som bearbetar signalerna innan dessa skickas vidare till fordonets elektroniska styrsystem. Det förekommer också att reglagen eller andra delar av fordonet används för att återföra information från andra system till föraren, till exempel vibrerande säten som varnar föraren för filbyten (Scania, 2017; Volvo, 2017). En konsekvens av denna utveckling är att fler system kommunicerar med varandra vilket ökar komplexiteten och därmed risken för cyberangrepp.

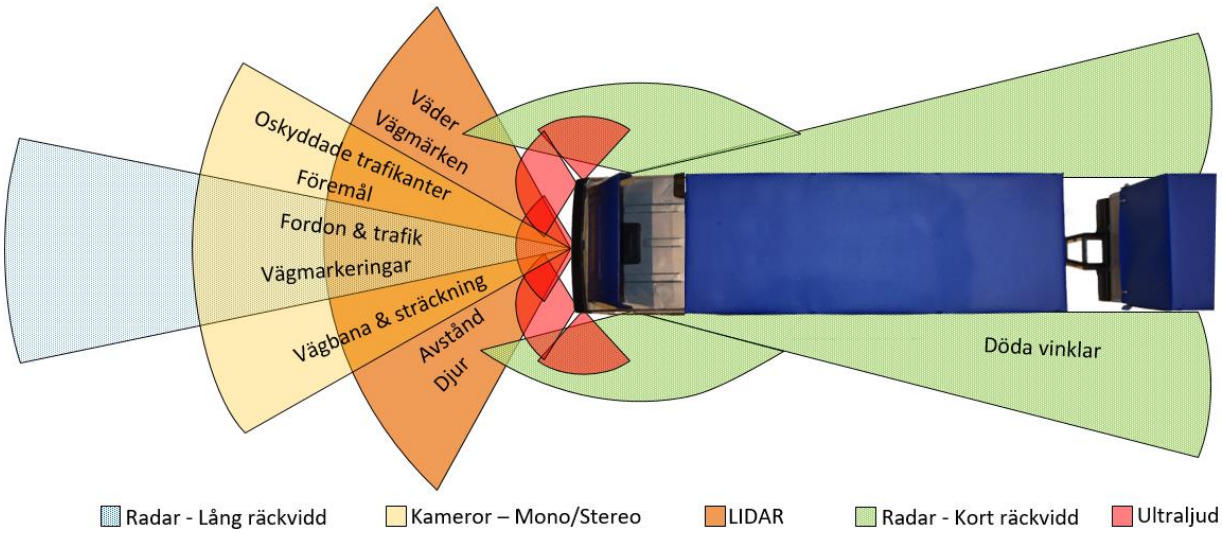
Värt att notera är att fysiska reglage i vissa fall ersätts helt med elektroniska reglage såsom pekskärmar. Dessa visar dynamiskt upp information som i flera fall har visats sig möjliga att förvanska med relativt enkla angrepp (Miller & Valasek, 2015). Samma forskning visar också att det via cyberangrepp är möjligt att påverka mekaniken i fordon genom att skicka elektroniska signaler men att föraren kan motverka effekten av angrepp genom att själv aktivt använda reglagen.

3.5 Sensorer

Sensorer är en viktig del av fordonets elektroniska styrsystem och tillhandahåller mätdata av olika slag. Fordonstekniska mätdata såsom temperaturer, tryck och avgasvärden samt säkerhetsinriktade mätdata såsom indikator för användning av säkerhetsbälte, alkomätare och varning för öppna dörrar har används länge inom fordonsindustrin. Dessa sensorer är idag allmänt förekommande i tunga fordon och trots att de flesta insignaler är begränsade till en viss del av fordonets kommunikationsbussar så finns det vissa mätdata som används i flera system[7].

En annan grupp av sensorer som visas i Figur 4 har till uppgift att tillhandahålla mätdata om fordonets omgivande miljö (Audi Technology Portal, 2018; Chamoun, 2014). Dessa sensorer används för styrsystem som i första hand inriktar sig på att förenkla förarens arbetssituation och för att ytterligare öka trafiksäkerheten. Denna grupp av sensorer kan redan idag påverka framförandet av fordonet och mätdata från dem är en förutsättning för utvecklingen inom autonoma fordon. Det förekommer också diskussioner om hur olika sensorer skulle kunna användas inom nya användningsområden, till exempel för att avvärja nyttjandet av tunga fordon vid terrorangrepp (SVT, 2017). Att dessa sensorer kan ha direkt påverkan på framförandet av fordonet gör dem intressanta ur ett cybersäkerhetsperspektiv.

[5] Systemexpert, Scania, Telefonintervju 2017-12-15
[6] Systemexpert, Östgötatrafiken, Telefonintervju 2017-12-19
[7] Systemexpert, Scania, Telefonintervju 2017-12-15



Figur 4: Sensorer som mäter fordonets omgivning och som sedan kan användas för att kontrollera framförandet av fordonet. Olika tillverkare använder olika sensorer för att åstadkomma bilden av omgivningen och ofta används flera olika sensortyper.

Sensorernas räckvidd och förmåga att upptäcka olika föremål varierar och därför används flera olika typer av sensorer för att åstadkomma en så korrekt bild som möjligt av omgivningen. Vilka sensorer som används, antal sensorer av varje typ och deras placering varierar stort mellan olika tillverkare. Ofta finns det flera sensorer av respektive typ på ett fordon, till exempel radarsensorer med olika våglängd, antennutformning och riktning (Chamoun, 2014).

Användningen av sensorer på tunga fordon kompliceras av att sensorerna generellt bara placeras på själva dragbilen (beroende på vem som äger släpet) vilket medför att mätområdet begränsas av det släp som dras. Detta har medfört att lastbilarnas backspeglar ofta används för att placera bakåtseende sensorer.

3.5.1 Lidar

Lidar (eng. Light detection and ranging) är en teknologi som använder laserljus för att mäta avstånd till ett föremål. Detta sker i princip genom att man skickar ut en ljuspuls och mäter tiden det tar innan reflektionen kommer tillbaka. Lidarsensorer kan använda allt från enstaka strålar som mäter avståndet till enskilda föremål till arrayer som ger en bild av ett område runt fordonet.

En fördel med lidar är att strålarna har en smalare spridningsvinkel än till exempel radar och att det därmed är möjligt att åstadkomma en mer detaljerad bild. En nackdel är att lidar påverkas mer av väderförhållanden såsom regn, snö och dimma samt att det är skadligt för ögonen varför signalstyrkan måste begränsas (Rudolf, Gert och Voelzke, Uwe 2017).

3.5.2 Radar

Radar använder radiovågor med olika våglängd för att mäta avstånd till (och upptäcka förekomsten av) ett föremål. Genom att anpassa effekt, våglängd och antennens utformning är det möjligt att anpassa radarsensorn för olika ändamål.

En fördel med radar är att den är mindre känslig för väderförhållande än till exempel kameror och lidar men den kan bara ge en ”grövre” bild över omgivningen (Rudolf & Voelzke, 2017).

3.5.3 Kameror

Kameror används för att samla in ljus som sedan analyseras för att åstadkomma en bild av fordonets omgivning. Användandet av kameror varierar mellan olika tillverkare och det finns monokameror med

endast en ljusöppning och stereokameror med två eller flera ljusöppningar. Fördelen med de senare är att de kan användas för att ”se” djup. Det är också möjligt att använda våglängder som inte kan ses av det mänskliga ögat (såsom IR och värmekameror) för att detektera föremål.

En fördel med att använda kameror är att de kan åstadkomma en detaljerad bild av omgivningen men nackdelar är att de är känsliga för väderförhållanden samt att det är ganska komplicerat att bearbeta all information i bilden som kamerorna genererar (Rudolf & Voelzke, 2017).

3.5.4 Ultraljud

Ultraljud skickar likt lidar och radar ut en aktiv signal och mäter hur lång tid det tar innan den kommer tillbaka. Våglängden medför att detektionsavståndet är begränsat (ofta till ett fåtal meter närmast fordonet) och dessa sensorer används därför primärt vid låga hastigheter.

Fördelar med ultraljudssensorer är att de är relativt billiga. Nackdelar är att de har kort räckvidd samt att de endast kan upptäcka föremål som reflekterar ljudet. (Rudolf & Voelzke, 2017).

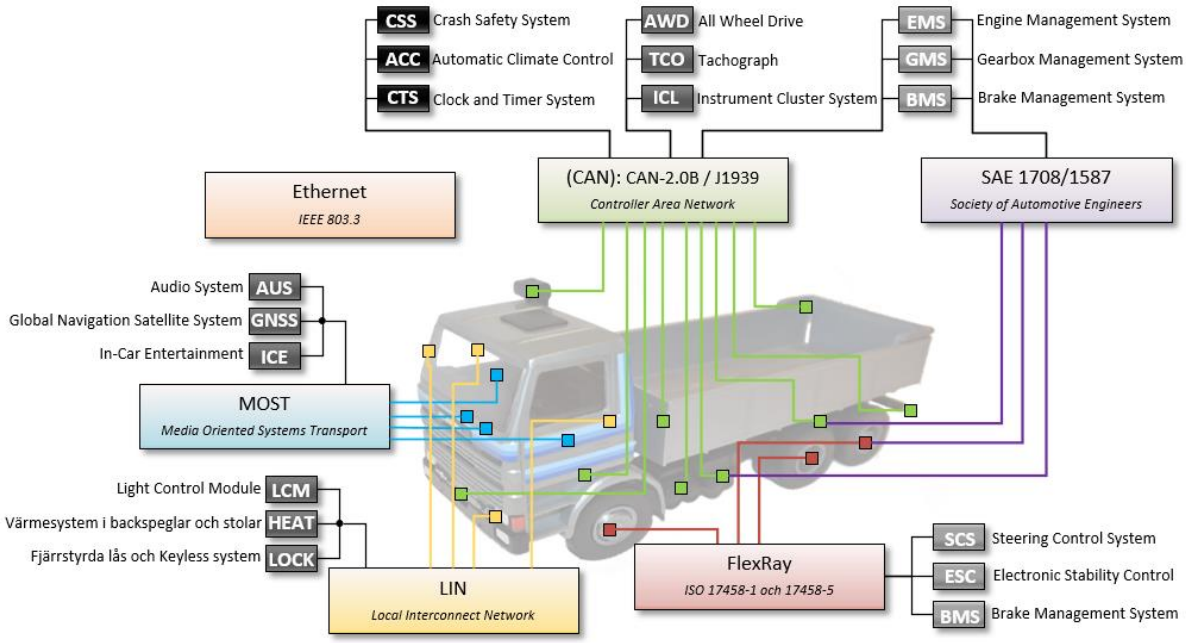
4 Kommunikation i fordon

Ett modernt tungt fordon kräver elektronisk kommunikation för att fungera och kommunicerar idag med ett flertal olika komponenter och system både i och utanför fordonet. Syftet med denna kommunikation är dels att fordonets interna system skall kommunicera med varandra för att höja säkerheten och göra fordonet mer effektivt, dels att på distans kunna övervaka fordonet och samla in diagnostisk data. Även om det finns ett antal olika nätverksprotokoll som används är det vanligt att olika system ansluts till en gemensam kommunikationsbuss.

4.1 Intern kommunikationsarkitektur

Till en början hade varje elektroniskt styrsystem i tunga fordon separata kabelsystem vilket ökade kostnaden, komplexiteten och vikten på fordonen. 1986 släpptes nätverksprotokollet CAN vilket medförde att de elektroniska styrsystemen kunde använda en gemensam kommunikationsbuss (CAN-wiki, 2016).

Sedan dess har behovet av ökad överföringskapacitet, krav på förbättrad realtidsfunktionalitet, säkerhet och skalbarhet lett till att CAN har kompletterats med flera nätverksprotokoll. Så även om man fortfarande talar om ”kommunikationsbussen” är det troligt att det i realiteten rör sig om flera olika kommunikationsbussar och nätverksprotokoll. I Figur 5 visas ett exempel på nätverksprotokoll och hur de kan användas i ett modernt tungt fordon (Vector, 2017; Johansson et al., 2005; Currie, 2015).



Figur 5: Nätverksprotokoll i ett modernt tungt fordon och ett exempel på hur de kan användas. Observera att användningen varierar med tillverkare, modell och tillverkningsår.

Observera att Figur 5 endast är ett generaliserat exempel på en tänkbar användning av olika nätverks-protokoll. Vilka protokoll som används och hur system och komponenter tillåts utbyta styrsignaler varierar med tillverkare, modell och tillverkningsår.

Tabell 1 ger en överblick över protokollen som idag används inom fordonsindustrin och dessa presenteras utförligare under respektive rubrik nedan. Tabellen har sammanställts från ett antal källor på internet som har identifierats genom att söka på respektive egenskap och protokoll. Ofta har olika källor haft motstridiga uppgifter om till exempel överföringskapacitet eller antal noder och tabellen är därför ett resultat av en värdering av dessa sökningar. En svårighet med att fylla tabellen med information har varit att överförings-kapacitet, noder och kabellängder inte är deterministiskt fastställda för flera av protokollen utan beroende av varandra.

Tabell 1: En jämförande tabell mellan några vanliga nätverksprotokoll i tunga fordon. Kolumnen ”Data” anger den maximala storleken på datafältet som respektive protokollet kan skicka. Förklaringen till tabellen presenteras nedan.

	Användning	Övergörings-kapacitet	Kabellängd	Noder	Data	Media	Kollisionskontroll
CAN/ISO 11898	Generell arkitektur	1 Mbps [1]	40 m [1]	30 st [2]	8 bytes	Dubbeltråd koppar [3]	CSMA/CD+AMP [4]
CAN FD	Generell arkitektur	~8 Mbps [1]	~40m [1]	30 st [2]	64 bytes	Dubbeltråd koppar [3]	CSMA/CD+AMP [4]
SAE J1708/1587	Generell arkitektur	9,6 kbps [1]	40 m [1]	20 st [5]	21 bytes	Dubbeltråd koppar [3]	Oklart
SAE J1939	Generell arkitektur	500kbps [1]	40 m [1]	253 st	1785 bytes	Dubbeltråd koppar [3]	CSMA/CD+AMP [4]
FlexRay	Kritiska komponenter	10 Mbps[6]	24 m	22 st	254 bytes	Dubbeltråd koppar [3]	TDMA [7]
LIN	Icke-kritiska komponenter	20 Kbps	40 m	16 st	8 bytes	Enkeltråd koppar	Polling
MOST	Multimedia	150 Mbps	15 m	64 st	372 bytes	Enkeltråd fiber eller koppar [8]	TDM samt CSMA [9]
Ethernet	Framtida användning	10 Gbps+ [10]	- [10]	- [10]	~1500 bytes	Enkeltråd fiber eller koppar	CSMA/CD

[1] Överföringskapacitet är direkt beroende av kabellängden och det som anges i tabellen är maximal kabellängd för angiven överföringskapacitet. CAN-nätverk har till exempel en teoretisk maximal kabellängd på 6000 meter vid överföringskapacitet på upp till 1 kbps.

[2] I standarden anges 30 noder som maximum men det finns många exempel på installationer med flera noder.

[3] Protokollet använder som standard två parallella koppartrådar som normalt användas för redundans. Varje nod ansluts då till båda trådarna i enlighet med Figur 6.

[4] Noden lyssnar på kommunikationsbussen, kontrollerar att den har varit inaktiv (att ingen annan nod har skickat data) och väntar under en förutbestämd period innan den sänder. Om kollision sker ändå ges prioritet till den mest kritiska kommunikationen.

[5] Protokollet verkar inte föreskriva något maximalt antal noder men rekommenderat antal enligt sökning på internet är mellan 10 och 20 noder per segment.

[6] Båda kanalerna kan vid behov istället användas som databärare vilket gör att FlexRay kan nå en maximal överföringskapacitet på 20 Mbps, men då försvinner redundansen i installationen.

[7] Nodernas kommunikation kontrolleras med en gemensam tidssynkronisering vilket minskar sannolikheten för kollisioner. Detta medför att FlexRay har högre tillförlitlighet än till exempel CAN och att redundansen är mindre känslig för högt utnyttjande av överföringskapaciteten.

[8] MOST byggs i en ringstruktur och kommunikationen passerar varje nod i ringen.

[9] Kollisionskontrollen beror på hur kommunikationen är uppsatt och kan använda token[8], TDM samt CSMA.

[10] Ethernet utgörs av en stor samling olika protokoll med olika funktioner och prestanda. Nätverken byggs företrädesvis i så kallad stjärntopologi och det finns flera olika typer av redundansprotokoll som kan

[8] Kan enkelt beskrivas som en signal på kommunikationsbussen som indikerar att det är ok att sända.

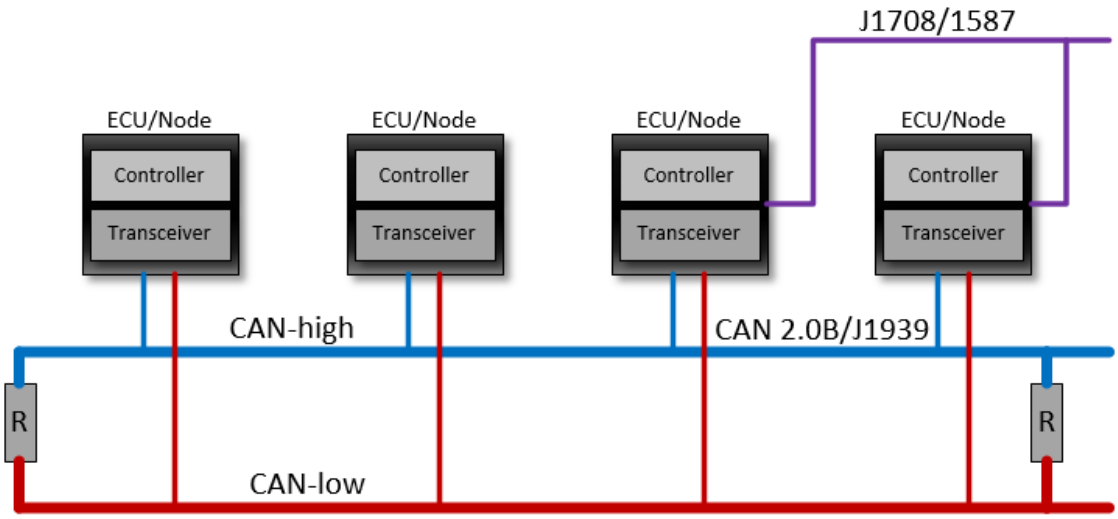
användas. Kabellängd och antal noder varierar beroende på vilken typ av media och vilken hastighet som används.

I resterande del av detta kapitel redovisas en översikt av de protokoll som tas upp i Tabell 1.

4.1.1 CAN/ISO 11898

Controller Area Network eller CAN är ett nätverksprotokoll som utvecklades av Bosch och standardiserades 1986 som ISO 11989 (CAN-wiki, 2016). Utvecklingen av standarden leds fortfarande av Bosch och en vanlig version av CAN-protokollet är CAN 2.0B. Enligt OSI-modellen definierar CAN 2.0B det fysiska lagret och datalänklagret. För övriga lager används andra nätverksprotokoll såsom CANopen eller SAE J1939 (Axiomatic, 2006; CiA, 2018).

I Figur 6 visas en skiss av en CAN-implementation med seriell kommunikation över två parallella bussar (CAN-High och CAN-Low). CAN-standarden definierar hastigheter upp till 1 Mbps. CAN-Low kallas ofta för låghastighetsbuss och säkerställer redundans i systemet i och med att kommunikation fortfarande är möjlig även om den ena kommunikationsvägen fallerar. I figuren används protokollet J1939 över CAN-bussen och protokollet J1708/1587 används för att tillhandahålla redundans åt kritiska system (Axelsson et al. 2003).



Figur 6: Ett exempel på en implementation av en CAN-buss med CAN-high och CAN-low samt protokollet SAE j1939. SAE 1708/1587 används i detta exempel för att åstadkomma redundans för kritiska system. R är resistorer som sitter mellan CAN-slingorna.

CAN-protokollets överföringskapacitet påverkas av längden på kabeln i CAN-bussen. Överföringskapacitet är något för begränsad för vissa tillämpningar, såsom infotainmentsystem. Standarden erbjuder ett tillförlitligt protokoll men saknar i övrigt funktioner för cybersäkerhet, såsom meddelandeautentisering (CAN-wiki, 2016).

2014 gav Bosch ut kompletteringen CAN FD som stödjer en överföringskapacitet på upp till 8 Mbps (CiA, 2018).

4.1.2 SAE J1708/1587

SAE International är en organisation som bland annat definierar standarder för fordonsindustrin. SAE J1708 är en standard som används för seriell kommunikation mellan styrsystemskomponenter i tunga fordon. J1708 definierar det fysiska lagret och datalänklagret av OSI-modellen. SAE J1587 är den standard som representerar ovanliggande protokoll till J1708 (transport- och applikationslager). J1587 definierar formatet och parametrarna på de meddelanden som skickas mellan komponenter i tunga fordon (Axelsson et al., 2003).

I dag har J1708/J1587 i hög grad ersatts av J1939 som baseras på CAN, men standarden används fortfarande i äldre fordon och för att åstadkomma redundans för kritiska system i nyare fordon (CSS Electronics, 2018).

4.1.3 SAE J1939

SAE J1939 är en standard som utvecklats av SAE International för att ersätta J1708/J1587 och som används i många tunga fordon, däribland Volvo och Scania (Scania, 2014; Axelsson et al., 2003). J1939 definierar protokoll för fem lager enligt OSI-modellen och utnyttjar det fysiska lagret som definieras i CAN-buss/ISO 11898. J1939 stödjer hastigheter på upp till 500 kbps och definierar utöver kommunikation också dataformat för utbyte av styrinformation för dieselmotorer. Standarden kan anses allmänt förekommande i moderna tunga fordon. Det finns flera ISO-standarder som är baserade på J1939 såsom ISO 11783 för skogs- och jordbruksmaskiner och ISO 11992 för släp för tunga fordon (Vector, 2017).

J1939 innehåller funktioner för robust kommunikation men denna påverkas negativt vid högre utnyttjande av överföringskapaciteten. Standarden saknar i övrigt funktioner för cybersäkerhet, såsom meddelandeautentisering (Vector, 2017).

4.1.4 FlexRay

FlexRay-konsortiet grundades i början av 2000-talet av bland annat BMW AG, Volkswagen AG, Daimler AG och General Motors. FlexRay-protokollet designades för att vara snabbare och mer pålitligt än CAN men är samtidigt mer kostsamt. Första implementationen av FlexRay i ett fordon kom 2006 i BMW X5 men det implementerades fullt ut först 2008 i BMW 7-serien. FlexRay-konsortiets arbete resulterade i ISO-standarderna 17458-1 till 17458-5 (Vector, 2017). Det är oklart huruvida Scania och Volvo använder FlexRay.

Som nämnt ovan har FlexRay högre överföringshastighet än CAN och är mer robust på grund av dess funktion för kollisionskontroll. FlexRay förväntas dock inte vara en ersättare till CAN, istället används det som ett komplement i säkerhetskritiska delar av fordonet som kräver realtidsfunktionalitet och redundans (Vector, 2017). Inte heller FlexRay har några egentliga funktioner för cybersäkerhet.

4.1.5 LIN

LIN (Local Interconnect Network) är ett seriellt nätverksprotokoll som används inom fordonsindustrin. Protokollet har, jämfört med FlexRay och CAN, en låg dataöverföringshastighet (20-40 kbps) och är framtaget som ett billigare alternativ för system med lägre krav på robusthet och prestanda. LIN används därför för delsystem av icke-kritisk natur som inte kräver överföring av större mängder data. Exempelvis används detta protokoll för elektroniskt styrda backspeglar och säten (Vector, 2017; Axelsson et al., 2003).

Protokollet saknar funktioner för cybersäkerhet, såsom meddelandeautentisering.

4.1.6 MOST

Media Oriented Systems Transport (MOST) är ett multimediaprotokoll med högre överföringshastighet än CAN/ISO 11898, J1939 och FlexRay. Protokollet används för video, audio, röst och liknande datasignaler i fordon. MOST används av en stor majoritet av alla fordonstillverkare i världen, till stor del på grund av dess anpassningsbarhet och plug-and-play-integration. Som nämnts under avsnittet CAN/ISO 11898 lämpar sig inte CAN-protokollet inte för infotainmentsystem då det har en för begränsad överföringskapacitet. Därför lämpar sig MOST-protokollet som ersättare till CAN/ISO 11898 för de delar av kommunikationsbussen som måste hantera mer nätverkstrafik (Vector, 2017; Axelsson et al., 2003).

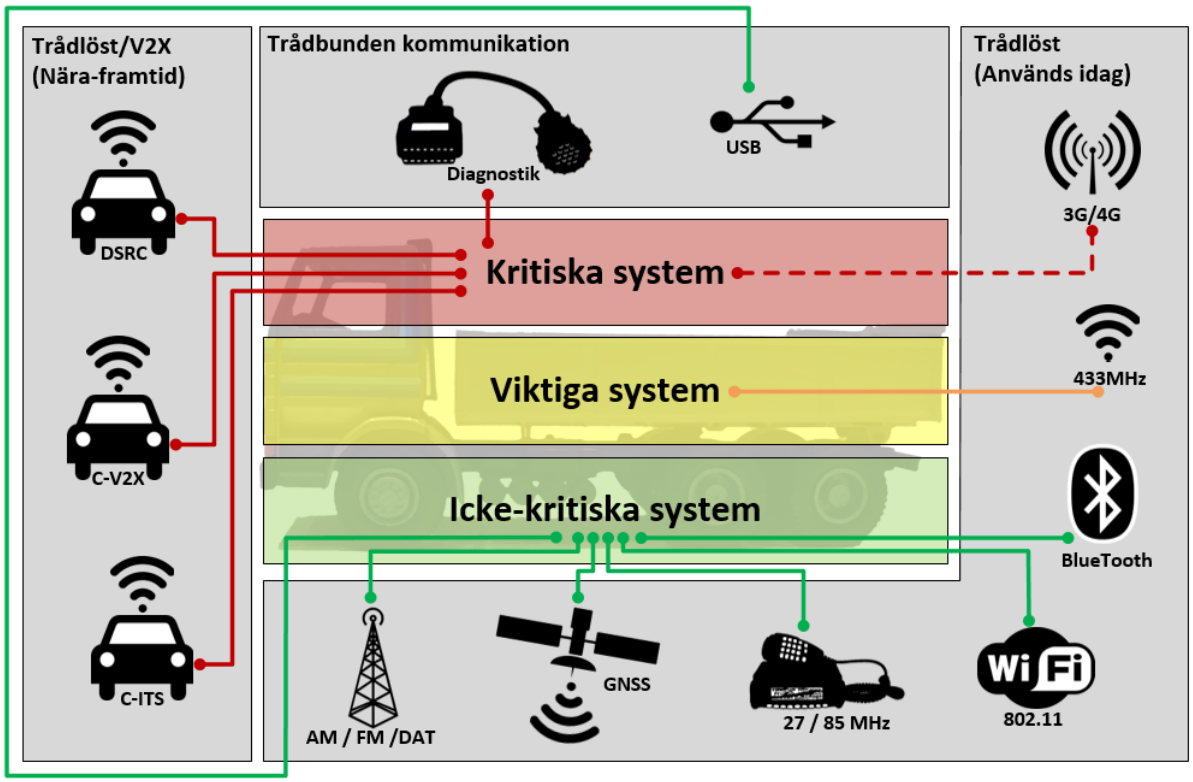
Inte heller MOST-protokollet erbjuder några egentliga cybersäkerhetsfunktioner.

4.1.7 Ethernet

Ethernetkommunikation för fordon är något som idag är attraktivt för fordonsindustrin och som troligtvis kommer att bli en nödvändighet i framtidens mer avancerade assisterande förarsystem. Det är en mogen standard med flera möjliga användningar inom fordonsindustrin. Detta på grund av den begränsade skalbarhet och överföringskapacitet som ges med existerande arkitektur (CAN, LIN MOST etc.) och den förhållandevis stora överföringshastighet som kan uppnås med Ethernet. En övergång till Ethernet skulle också göra det möjligt att snabbt implementera många av de cybersäkerhetsmekanismer som protokollet och dess tillhörande protokoll på högre OSI-nivåer (såsom TCP/IP) erbjuder (Vector, 2017).

4.2 Extern kommunikation i fordon

För att fordonet skall kunna kommunicera med omvärlden krävs ytterligare protokoll och komponenter utöver de som nämns ovan. Vilka dessa är varierar beroende på vilken typ av kommunikation som avses. I Figur 7 visas de externa kommunikationsteknologier som används i dagens tunga fordon med fokus på typiska användningsområden (Vector, 2017; Axelsson et al., 2003; Johansson et al., 2005).



Figur 7: En översikt över externa kommunikationsteknologier som används i moderna tunga fordon och vilka typer av system de typiskt ansluts till. Notera att det ofta förekommer flera implementationer av respektive teknologi.

Figuren är en förenkling och i verkligheten kan det finnas flera implementationer av varje teknologi. Beroende på hur den interna kommunikationsarkitekturen ser ut, kan de externa kanalerna medföra cybersäkerhetsrisker för fordonet. Ett särskilt problem förefaller dock vara inkopplingen av mobilkommunikation (3G/4G), framförallt om kommunikationen ansluts till fordonets diagnostikuttag då detta uttag exponerar känsligare system[9]. En annan viktig aspekt som bör beaktas är huruvida de enheter som använder dessa kommunikationsteknologier i fordonet i sin tur skyddas samt hur kommunikationssystemen uppdateras regelbundet för att hantera cybersäkerhetshot. Exempel på relevanta

[9] Systemexpert, Scania, Telefonintervju 2017-12-15

hot att beakta är till exempel BlueBorne och Krack som angrep Bluetooth respektive WiFi (Armis, 2017; Vanhoef & Piessens, 2017).

Observera att nedanstående beskrivning av kommunikationsteknologierna avsiktligt sker på en överskådlig nivå och med fokus på hur dessa används i tunga fordon. För utförligare information om respektive teknologi hänvisas till annan dokumentation.

4.2.1 Diagnostikuttag

Diagnostikuttagen i fordon utgör en särskilt intressant anslutningspunkt ur ett cybersäkerhetsperspektiv eftersom dessa uttag används för uppdatering av all mjukvara på ECU:erna i fordonet (Scania Truck Bodybuilder, 2016). Uppdateringar sker normalt via särskilda enheter på verkstaden men det förekommer tredjepartsutrustning med 3G/4G-modem på marknaden som ansluts direkt till dessa uttag, vilket torde medföra att en osäker uppkoppling skapas direkt till den interna kommunikationsbussen i fordonet.

4.2.2 WiFi

Det blir allt mer vanligt att fordon har egna WiFi-uppkopplingar för att passagerare skall få tillgång till internet. För att detta skall fungera krävs att fordonet har ett 3G/4G-modem installerat. Om inte denna kommunikation är isolerad från den interna kommunikationsbussen kan denna kommunikationsväg missutnyttjas av individer i fordonets närhet för att få tillgång till den interna kommunikationsbussen i fordonet (Checkoway et al., 2011).

4.2.3 Bluetooth

Bluetooth har använts inom fordon i flertalet år för att ge förare och passagerare möjlighet att koppla sina mobiltelefoner och andra enheter till fordonets infotainmentsystem och genom det kunna ta emot samtal, SMS eller lyssna på musik (Checkoway et al., 2011).

4.2.4 3G/4G

3G/UMTS[10] och 4G/LTE[11] har många användningsområden inom fordon, dels kan det användas av passagerare och förare för extern kommunikation över internet, dels används det av fordonet självt för att kommunicera med andra fordon och centrala system hos tillverkaren. Specifikt för tunga fordon används även 3G/4G för FMS-kommunikation, där diagnostiskdata för fordonet och färdskrivardata för föraren skickas till ett centralt system hos tillverkare som i sin tur kan nås från ägaren (Checkoway et al., 2011).

3G/4G används också av många tredjepartssystem för att ge åtkomst till fordonet.

4.2.5 Radiokommunikation

Det används en rad olika radiokommunikationsprotokoll i tunga fordon. Bland annat FM-/AM-radio, komradio på 27/85Mhz för förarkommunikation och LPD433[12] för nyckellås och däcktryckssystem. De två tidigare har använts under lång tid och påverkar främst icke-kritiska system i fordonet. LPD433 bör dock beaktas som en möjlig cybersäkerhetsrisk då det dels påverkar viktigare system och dels eftersom det finns exempel på forskning där man har lyckats angripa fordon just via denna kanal (Checkoway et al., 2011).

[10] Universal Mobile Telecommunications System
[11] Long Term Evolution
[12] Low Powered Device 433 MHz

4.2.6 Global Satellitnavigering

Det finns två primära användningsområden för GNSS[13] i fordon: platsspårning av fordonet och vägbeskrivningar för fordonets färd. Både fordonets interna system och externa enheter kan användas för dessa ändamål. Det blir dock allt vanligare att dessa system inkluderas i själva fordonet för att inte behöva förlita sig på tredjepartsystem. Detta eftersom att det är svårt för en tillverkare att ta hänsyn till och skydda sig från implikationer av ett tredjepartsystem på den interna kommunikationsbussen. Å andra sidan behöver de tredjepartssystem som används sällan kopplas in på den interna kommunikationsbussen då enheten inte behöver hämta information från något av fordonets interna system (Checkoway et al., 2011).

GNSS-spårning används även inom andra system för tunga fordon, så som FMS, vilket ger ytterligare argument för implementation och användande av ett internt GNSS-system.

4.2.7 V2X

V2X refererar till en kommunikationsarkitektur där fordon, infrastruktur och andra påverkande objekt sammankopplas och kommunicerar med varandra. Detta är till stor del en framtidsvision, men det finns vissa implementationer av detta redan idag. Exempelvis i systemet Volvo Connected Truck som möjliggör distansdiagnostik av fordonets kritiska funktioner, bränsleförbrukning och miltal. Föraren har även möjlighet att via en mobilapplikation se status för vissa komponenter i fordonet såsom batteristatus, bränslenivå och oljenivå. Applikationen meddelar även föraren om inbrottslarmet utlöses (Volvo, 2017).

Vissa tillverkare har även utvecklat system för V2V (Vehicle-to-Vehicle) där ett fordon kommunicerar med ett annat fordon. Ett exempel på ett sådant system är Volvos Connected Safety vilket kan detektera halt väglag och varna föraren av fordonet men även förare av andra fordon i närheten som har Connected Safety aktiverat. Liknande system finns för andra leverantörer exempelvis Scania Connected Services (Volvo, 2017; Scania, 2017).

Begreppet V2X kan definieras som all kommunikation som går från fordonet och sträcker sig utanför gränsen för fordonet, det vill säga kommunikation mellan ett fordon och en utomstående motpart. Ett exempel på detta är kommunikation som sker mellan fordonet och andra fordon under färd, eller mellan fordonet och infrastruktur det möter längs vägen. Dessa motparter är inte i förväg definierade i den bemärkelse att fordonet inte på förhand kan veta vilka andra fordon eller vilken infrastruktur det kommer att möta under färden (Slovick, 2017).

Det pågår ett arbete hos flera företag, organisationer och fordonstillverkare med att utveckla och testa implementationer av V2X för storskaligt bruk. En viktig grund för all V2X-funktion är standardiserade kommunikationsmetoder och just nu utvecklas C-ITS (Cooperative Intelligent Transport Systems), DSRC (Dedicated Short-Range Communications) och C-V2X (Cellular Vehicle-to-everything) av olika aktörer. Teknologierna som används skiljer sig mellan de olika initiativen, även om alla har ett gemensamt primärt mål; att förbättra trafiksäkerheten och för att åstadkomma detta behövs ofta att kommunikationen leder till en automatisk åtgärd som påverkar fordonet, till exempel autobromsning (Slovick, 2017). Detta, tillsammans med det faktum att motparten är okänd, gör systemen speciellt utmanande ur ett cybersäkerhetsperspektiv.

4.2.7.1 C-ITS

C-ITS (även kallat ITS G5) eller är EUs motsvarighet till det amerikanska DSRC som är tänkt att lanseras på frekvensbandet 5,9 GHz under 2019. Räckvidden är < 500 m (Slovick, 2017).

4.2.7.2 DSRC

DSRC är en amerikansk standard för ett trådlöst kommunikationssystem ämnat för kommunikation mellan fordon och kommunikation mellan fordon och infrastruktur (Slovick, 2017).

[13] Global Navigation Satellite System

4.2.7.3 C-V2X

C-V2X från teleoperatörsindustrin, är en utmanare till DSRC som nyttjar existerande mobilkommunikation (4G/LTE och inom en snar framtid 5G). En möjlighet med denna teknologi är att man kan nyttja existerande infrastruktur och teknologi för att kommunicera med andra typer av enheter och intressenter, till exempel en fotgängare med en mobiltelefon (Slovick, 2017). Detta möjliggörs genom att den vanliga mobiluppkopplingen mellan enhet och basstation kompletteras med en länk som kallas PC5 eller side-link och som möjliggör korthållskommunikation (500–1000 m). Denna länk kan användas även utan kontakt med telenätet[14].

[14] Systemexpert, Ericsson, E-post, 2018-01-22

5 Diskussion

Målet med detta memo är att ge en överskådlig bild av de komponenter och teknologier som används för att bygga elektroniska styrsystem i tunga fordon, hur komponenterna kommunicerar med varandra och hur de kommunicerar med omvärlden. Efterforskningarna visar att det råder en viss begreppsförvirring inom industrin då tillverkare tenderar att använda egna förkortningar och namn på system. Det är också vanligt att man generaliserar teknologier, använder felaktiga begrepp och att samma eller liknande system hos olika tillverkare har helt olika namn. Detta försvårar dialogen mellan fordonstillverkare, komponent-tillverkare, fordonsoperatörer och tredjepartleverantörer vilket medför ökande cybersäkerhetsrisker eftersom gränsdragningen blir otydlig och risken för missförstånd ökar. Ett annat problem som framgår av våra efterforskningar är att systemen i tunga fordon tills nyligen inte har tagit hänsyn till cybersäkerhet och att man i viss mån inte heller är medveten om dessa problem inom branschen.

De teknologier och komponenter som används i tunga fordon överensstämmer i stort med den som finns i personbilar, men vissa protokoll, såsom SAE J1939, är specifikt framtagna för just tunga fordon.

De system och komponenter som återfinns i fordon har utvecklats med fokus på funktionell säkerhet och robusthet snarare än cybersäkerhet. Det har tidigare funnits ett begränsat behov av att utveckla dessa system med fokus på just cybersäkerhet, men i takt med att dessa system och fordonen i stort blir allt mer uppkopplade finns nu ett nytt behov av fokus på cybersäkerheten. De trafiksäkerhetsfunktioner som fordon utvecklas med har dock positiva effekter på cybersäkerhet. Specifikt gäller detta redundansen av system och komponenter i fordonet, att dessa fortsätter fungera även om kommunikationen bryts, samt att föraren alltid har den absoluta kontrollen över fordonet. En relevant frågeställning är dock, gällande exemplet från avsnitt 2.6, om föraren i en sådan situation kan reagera tillräckligt snabbt för att motverka påverkan från ett cyberangrepp.

Det finns även ett ökat medvetande kring cybersäkerhet inom fordonsindustrin idag, vilket har föranlett ett inkluderande av cybersäkerhetsarbete inom diverse utvecklande projekt, exempelvis inom V2X. Detta är en positiv utveckling sett till framtidens autonoma system där cybersäkerhet kräver en central roll, eftersom föraren då inte längre har möjlighet att ta kontroll över fordonet. Konsekvenserna av ett angrepp som lyckas ta över ett fordon har då potential att bli mycket värre än i dag då föraren inte längre har den absoluta kontrollen över fordonet. I takt med att V2X implementeras i stor skala till att inkludera allt fler enheter av olika typer krävs ett cybersäkerhetsrelaterat arbete för dessa enheter. Det krävs även analyser för att uppmärksamma vilka konsekvenser ett angrepp mot en enhet potentiellt kan få på övriga enheter i systemet, i synnerhet vilka konsekvenser det kan få för de fordon som verkar i systemet.

De protokoll som används idag för fordons kommunikationsbussar är precis som andra systemsystem utvecklade med fokus på funktionell säkerhet, redundans och robusthet. Det finns brister i dessa protokoll ur ett cybersäkerhetsperspektiv, exempelvis finns sällan någon autentisering av meddelanden vilket har potential att påverka säkerheten negativt då man inte kan veta vilket system som skickade meddelandet. Problemet med säkerhetsfunktioner i denna kontext är att de kan introducera fördröjning i kommunikationen vilket för system som kräver realtidsprecision inte är acceptabelt. Detta, i kombination med en redan begränsad överföringskapacitet kan skapa stora problem för hela fordonets säkerhet. Det finns potentiella lösningsförslag, som att exempelvis övergå till Ethernet-baserad kommunikation vilket löser problematiken med begränsad överföringskapacitet. Det krävs dock vidare forskning och utveckling för att hitta en tillfredsställande lösning på problemet.

Ett annat problem som till stor del påverkar tillverkare av tunga fordon är icke-auktoriserade tredjepartssystem. En del av tredjepartsleverantörerna går så långt att de tar bort instrumentpanelen för att komma åt kommunikationsbussen eller går via diagnostikuttaget i fordonet för att nå samma resultat. Problemet med detta kan påverka fordonets elektroniska styrsystem på ett sätt som varken tillverkaren, användaren eller tredjepartleverantören har avsett eller tänkt på. Riskerna med installation av sådana system kan vara katastrofala då de kan innehålla kod och funktioner som inte är kompatibla med fordonets egna system och då påverkar hela fordonets integritet och funktionalitet negativt. De kan även innehålla 3G/4G-uppkoppling vilket är en synnerligen stor risk då man dels har åtkomst till den interna

kommunikationsbussen, dels kan nå denna från distans genom fjärruppkoppling. Detta blir som en öppen inbjudan för angripare att ge sig på fordonet, vilket kan få stora konsekvenser.

Referenser

Armis (2017). *BlueBorne PROTECTING THE ENTERPRISE FROM BLUEBORNE*. Armis. White paper. http://go.armis.com/hubfs/BlueBorne%20Technical%20White%20Paper.pdf (Hämtad 2017-12-19)

Audi Technology Portal (2017). *Audi A8 - Audi AI traffic jam pilot*. Audi AC. https://www.audi-technology-portal.de/en/electrics-electronics/driver-assistant-systems/audi-a8-audi-ai-traffic-jam-pilot (Hämtad 2018-01-15)

Autoline (2018). http://autoline.info/-/electrics/trucks--c526fc2?mark_id=2742%3B2819 (Hämtad 2018-01-15)

Axelsson, J., Fröberg, J., Hansson, H., Norström, C., Sandström, K., Villing, B. (2003). *A Comparative Case Study of Distributed Network Architectures for Different Automotive Applications*. The Industrial Information Technology Handbook 1–17.

Axiomatic (2006). *Q&A – What is CAN.* Axiomatic. www.axiomatic.com/whatiscan.pdf Hämtad (2017-12-15)

CAN-wiki (2016). *Welcome to the CAN-bus Wiki project.* 2016-08-12. http://www.can-wiki.info/doku.php?id=can_faq:main Hämtad (2017-12-08)

Chamoun, J. (2014). *Traffic jam pilot app wins prestigious design award.* Scania. 19 augusti. http://www.scania.com/group/en/traffic-jam-pilot-app-wins-prestigious-design-award/ (Hämtad 2017-12-15)

Charette, R., N. (2009). *This car runs on code*. IEEE Spectrum. https://spectrum.ieee.org/transportation/systems/this-car-runs-on-code, 1 Feb. (Hämtad 2017-12-15)

Checkoway, S. Mccoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F., Kohno, T., (2011). *Comprehensive Experimental Analyses of Automotive Attack Surfaces*.

CiA, (2018). *CAN lower- and higher-layer protocols.* CAN in Automation. https://www.can-cia.org/can-knowledge (Hämtad 2018-01-11)

CSS Electronics, (2018*). SAE J1939 EXPLAINED - A SIMPLE INTRO (2018).* https://www.csselectronics.com/screen/page/simple-intro-j1939-explained/language/en (Hämtad 2018-01-09)

Currie, R. (2015). *Developments in Car Hacking*. The SANS Institute, 2015-12-05

Dittmer, J. (2001). *Are you ready for Drive-by-Wire.* Frost & Sullivan Market Insight. 14 november. http://www.frost.com/prod/servlet/market-insight-print.pag?docid=CEHR-54YTXP (Hämtad 2017-12-17)

Fleetboard (2018). *FleetBoard Sweden.* Daimler FleetBoard GmbH. http://www.fleetboard.se (Hämtad 2018-01-03)

FMS-Standard (2004). *Ivan Hodac. Secretary General. Subject: CAN bus connection.* http://www.fms-standard.com/Truck/down_load/letter_acea.pdf (Hämtad 2018-01-26)

Johansson, K.H., Törngren, M., Nielsen, L. (2005). *Vehicle Applications of Controller Area Network, Handbook of Networked and Embedded Control Systems*. Birkhäuser Boston, Boston, MA, ss. 741–765. doi:10.1007/0-8176-4404-0_32

Miller, C., Valasek, C. (2015). *Remote Exploitation of an Unaltered Passenger Vehicle*. Defcon 23 2015.

Rudolph, G., Voelzke, U. (2017). *Three Sensor Types Drive Autonomous Vehicles*. Sensors Online, Questex LLC. 10 november https://www.sensorsmag.com/components/three-sensor-types-drive-autonomous-vehicles (Hämtad 2018-01-02)

Scania (2014). *CAN-gränssnitt för påbyggnad*. Scania CV AB 2014, 22:10-078 Utgåva 1 2014

Scania Truck Bodybuilder (2016). *Allmänt om CAN*. Scania CV AB 2016, 22:10-753 Utgåva 1 2016-09-02

Scania (2017). *Säkerhetssystem. Scania Sverige AB*. https://www.scania.com/se/sv/home/products-and-services/articles/safety-systems.html (Hämtad 2017-12-19)

Slovik, M. (2017). *DSRC vs. C-V2X: Looking to impress the regulators.* ElectronicDesign, 2017-10-05

SVT (2017). *"Geofencing" ska hindra lastbilskapningar.* Sveriges television AB. 18 maj. https://www.svt.se/nyheter/inrikes/geofencing-ska-hindra-lastbilskapningar (Hämtad 2018-01-16)

Trakm8 (2011). *Trakm8 Install for FMS Volvo FM, FL, FH, FE*. Version 1.0: 21/08/11. Trakm8. 2011

(2) Trakm8 (2018). *Fleet management | Trakm8.* Trakm8 Limited. http://www.trakm8.com/fleet-management (Hämtad 2018-01-03)

Transportstyrelsen (n.d) *Fordonsregler.* http://www.transportstyrelsen.se/sv/vagtrafik/Fordon/Fordonsregler/ (Hämtad 2018-02-02)

Vanhoef, M., Piessens, F. (2017). *Key Reinstallation Attacks*. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security - CCS '17. ACM Press, New York, New York, USA, ss. 1313–1328. doi:10.1145/3133956.3134027

Vector (2017). *Welcome to the virtual VectorAcademy.* Vector Informatik GmbH. https://elearning.vector.com/vl_index_en.html (Hämtad 2017-12-15)

Volvo (2017). *Världens säkraste Volvo*. AB Volvo. http://www.volvotrucks.se/sv-se/trucks/volvo-fh-series/safety.html Hämtad (2017-12-19)