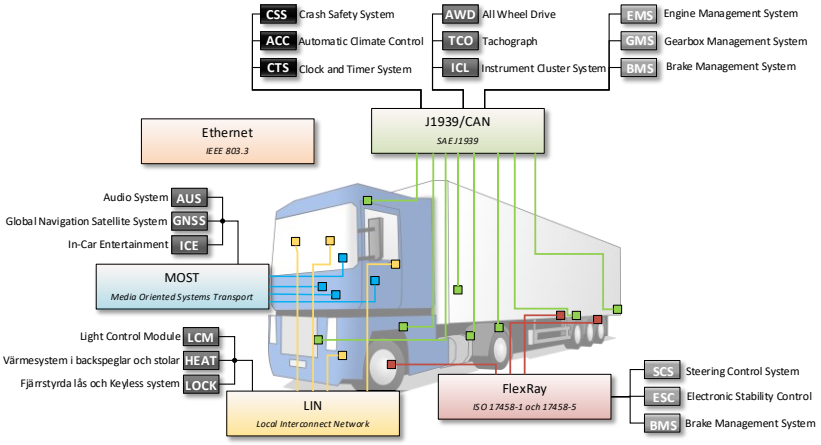
Faktablad

Avdelningen för cybersäkerhet och säkra kommunikationer
Enheten för säkerhet i cyberfysiska system
Publ.nr MSB1798 – juni 2021



Nätverksprotokoll i ett modernt tungt fordon och exempel på hur de används. Ett typiskt fordon kan ha 100 styrdatorer med 100 miljoner rader programkod.

Cyberfysiska sårbarheter i tunga fordon -

Med inriktning mot tunga fordon av vikt för civilt försvar

Den tunga vägtrafiken blir progressivt allt mer digitaliserad, både vad avser fordonen och den omgivande infrastrukturen. Antalet datorsystem i ett typiskt modernt tyngre fordon är redan stort och antalet radiouppkopplingar som installeras ökar vilket även ökar fordonens sårbarhet för cyberangrepp på distans. För MSB är denna utveckling av intresse då både räddningstjänst och samhällsviktig verksamhet som exempelvis livsmedelsförsörjning är beroende av denna typ av trafik.

Detta faktablad baseras på en studie[1] som MSB gav FOI i uppdrag att genomföra, denna baseras på literaturstudier och interviuer.

Kunskapsnivåer om cybersäkerhet

De huvudaktörer som har beaktats är tillverkare, påbyggnadsledet (som tar ett chassi och bygger om det för ett visst ändamål, exempelvis räddningstjänst), och användare/beställare. Kunskapsnivån hos beställare/användare anges vara låg, och utvärdering av cybersäkerhet saknas vid beställning av fordon. Det är oklart hur cybersäkerhet hanteras i beställningsprocessen för

Attackytor

Trådburen kommunikation och indirekt fysisk tillgång

Angriparen ansluter via av brukaren introducerade enheter som mobiltelefoner eller datorer anslutna till exempelvis diagnostikuttag eller multimedia-gränssnitt.

Trådlös kommunikation kortdistans

Normalt 1-100 meter men med modifierad antenn mm mycket längre, där hacker angriper exempelvis via fordonets Bluetooth, WiFi, eller TPMS (Tire Pressure Monitoring System)

Trådlös kommunikation långdistans

Avstånd i kilometer, där angriparen använder sig av exempelvis fordonets 3G/4G/5G, Over-the-air-uppdatering, Fleet Management System (FMS), och telematiksystem.

[1] FOI-R--5067--SE Cyberfysiska sårbarheter i tunga fordon ISSN 1650-1942

Kontakta oss:
Tel: 0771-240 240
registrator@msb.se
www.msb.se

Myndigheten för samhällsskydd och beredskap

kringutrustning, exempelvis bärbara datorer som används i fordonen, då denna sköts av andra kommunala instanser. Högst är kunskapsnivån i tillverkarledet.

Riskabel ombyggnation av fordon

Tredjepartssystem är system som är installerade i fordon av en leverantör som inte är originaltillverkaren. Dessa kan ha olika ändamål, den vanligaste är fordonsparksförvaltningssystem (eng. Fleet Management System (FMS)). Dessa 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 kan leda till att fordonets cybersäkerhetsåtgärder kringgås och kan påverka fordonets elektroniska styrsystem på ett sätt som varken tredjepartsleverantören, tillverkaren eller ägaren avsett eller insett.

Hotbild

Det har experimentellt visats att det går att påverka framförningen av tunga fordon exempelvis i syfte att försöka framkalla en trafikolycka. Detta kan genomföras via ett hackerangrepp på distans om fordonet har en internetuppkoppling över mobiltelefoninätet (exempelvis för infotainment) eller har annat radiogränssnitt som kan utnyttjas.

Det allvarligaste hotet mot tunga fordon är dock enligt studien tillgänglighetsangrepp; att fordon temporärt görs obrukbara exempelvis med ransomware, detta gäller så väl inom samhällsviktig verksamhet som kommersiell verksamhet.

Slutsatser

Fordonstillverkare har börjat tillämpa cybersäkerhetsprinciper vid nytillverkning, men generellt är cybersäkerheten låg för tunga fordon. Detta, i kompination med att attackytorna ökar, (exempelvis genom fler internetanslutningar), gör att risken för framgångsrika cyberangrepp ökar.

Den långa livslängden hos exempelvis fordon för räddningstjänst riskerar medföra att säkerhetsbrister kvarstår under lång tid, det är därför angeläget att så snart som möjligt höja beställarnas kompetens inom cybersäkerhetsområdet.

Kontakta oss:
Tel: 0771-240 240
registrator@msb.se
www.msb.se

MSB Myndigheten för samhällsskydd och beredskap