Vid korrespondens åberopa
FOI beteckning

Datum
2014-09-10

Dnr FOI-2014-967

Näringsdepartementet
103 33 Stockholm

Er referens
dnr (2013/4071/TE)

Vår handläggare
Jacob Löfvenberg

Remissvar gällande ”Nationell strategi och handlingsplan för användning av ITS”

Sammanfattning

Ett intelligent transportsystem (ITS) kan ses som samhällskritisk infrastruktur och måste utformas på ett sätt så att det tål att utsättas för både avsiktlig och oavsiktlig påverkan. FOI har funnit att remissen saknar åtgärder för detta i form av krav på säkerhet och robusthet. Dessa frågor är så viktiga att de explicit bör anges i den strategiska åtgärdslistan. Vidare menar FOI att tjänsteutveckling, interoperabilitet, hantering av publika data och innovationsupphandling skulle underlättas om de standarder som används för ITS-lösningar är öppna.

FOI föreslår att i Avsnitt 5, Strategiskt delmål 5, lägga till en åtgärd för att lyfta fram behovet av säkerhet och robusthet i framtida ITS-lösningar, samt att omformulera Åtgärd 5.1 för att tydligare efterfråga standarder som är öppna.

Bakgrund

FOI menar att en betydande andel av ITS kommer att vara beroende av trådlös teknik, både för kommunikationstjänster och för positionstjänster (t.ex. GPS). Civil trådlös teknik är i regel känslig för radiostörningssignaler. Dessa störningssignaler kan vara oavsiktliga och då härröra från egna samlokaliserade system, eller avsiktliga från exempelvis illegal användning av störsändare. Ett exempel är tillgången till billiga GPS-störsändare som ökat via internetförsäljning, och vars användning bland yrkesfordon regelbundet har uppmärksammats i internationella medier. FOI menar att i kritiska ITS är skydd mot radiostörning nödvändigt.

Tekniken i ITS förutsätter regelbunden försörjning av uppdaterad digital information från andra system, t.ex. i form av kartor. Sådan försörjning kan inte garanteras, bl.a. beroende på avsiktlig störning, dålig radiotäckning eller andra kommunikationsproblem. Det kan konstateras att ITS behöver dels diagnosfunktioner för att identifiera dataförsörjningsproblem, dels robusthet i transportsystemen så att de kan fungera säkert trots sådana problem.

Varje ITS innehåller ett eller flera IT-system av något slag, i allmänhet anslutet till andra datanät. Att dessa IT-system kanske inte ser ut som ”vanliga” datorer, utan är inbyggda eller utgör ett styr- och kontrollsystem påverkar inget i sak. Dessa system är känsliga på samma sätt som ”vanliga”

FOI
Totalförsvarets forskningsinstitut

Postadress	Besöksadress	Telefon	Fax	registrator@foi.se
FOI 164 90 STOCKHOLM	Gullfossgatan 6, Kista Leveransadress Gullfossgatan 12, Kista	08-55 50 30 00	08-55 50 31 00	Orgnr: 202100-5182 www.foi.se

datorer, något som exemplifieras av datamasken Stuxnet som upptäcktes 2010. Stuxnet anses ha haft som syfte att sabotera Irans kärnvapenprogram genom att störa styrsystemet i urananrikningsanläggningen i Natanz. FOI vill peka på att intelligenta system baserade på nätansluten IT är mycket känsliga för extern påverkan i form av IT-attacker. Rapporter om nya intrång återkommer ofta, även i allmänna medier. Typiskt för effekterna av dessa störningar är att de mycket plötsligt kan bli omfattande trots en lång tid av normal funktion. FOI menar därför att ITS som är kopplade till datanät bör förses med skydd mot IT-attacker.

Varje ITS kommer att realiseras i form av en fysisk, teknisk implementation i form elektrisk och elektronisk utrustning (datorer, kablage, sensorer, radioutrustning med mera). Skador på denna utrustning riskerar att allvarligt påverka funktionen hos det eller de ITS som utrustningen stödjer. Av detta skäl menar FOI att den utrustning som realiserar ett ITS bör förses med tillräckligt skydd mot fysisk påverkan.

Utredningen pekar på tre viktiga områden som måste hanteras för att få externa aktörer att utveckla de tjänster som resenärer efterfrågar: nya affärsmodeller, interoperabilitet och hantering av publika indata. Vidare pekas innovationsupphandling ut som ett viktigt medel för att nå transport- och innovationspolitisk måluppfyllelse. FOI anser att för att underlätta tjänsteutveckling, interoperabilitet, hantering av publika data samt för att möjliggöra innovationsupphandling, krävs öppna standarder för ITS-lösningar.

Avsnitt 5, ”Strategi och handlingsplan för ITS”

I underavsnittet ”Strategiskt delmål 5: ITS ska i första hand utvecklas genom att utnyttja befintlig digital infrastruktur” beskrivs fyra åtgärder för utvecklingen av ITS. Ingen av åtgärderna innehåller skrivningar om säkerhet eller robusthet för de ITS som ska utvecklas. Detta är olyckligt eftersom funktionsstörningar i ett allmänt använt, effektivt och välfungerande ITS kan antas ge omfattande störningar på de transporter som stödjs av systemet, eller för ett säkerhetskritiskt ITS till och med skador på liv och egendom.

Ett förslag är att lägga till ytterligare en åtgärd:

Åtgärd: *Säkerställ att ITS-lösningar har en adekvat robusthet mot avsiktlig och oavsiktlig påverkan.*
Kommentar:

- *de ITS som använder trådlösa system för kritiska tjänster ska adressera sårbarhetsaspekter för både avsiktliga och oavsiktliga radiostörningar*
- *ITS kopplade till datanät ska ha tillräckligt skydd mot IT-attacker*
- *de ITS som behöver regelbunden informationsförsörjning från andra system ska kunna hantera bortfall i denna försörjning*
- *fysiska hot och skydd för ITS-lösningarna ska beaktas*

Ett förslag är att omformulera Åtgärd 5.1 till:

Säkerställ användande av i första hand nationellt och internationellt beprövade ITS-lösningar med öppna standarder. Undvik parallella utvecklingsspår.

FOI

Datum
2014-09-10

Nr
FOI-2014-967

Detta remissvar har beslutats av undertecknad, överdirektör Anna-Lena Österborg, efter föredragning av laborator Jacob Löfvenberg.

För FOI,

Anna-Lena Österborg

Jacob Löfvenberg