Vain alkuperäiset UNECE:n tekstit ovat kansainvälisen julkisoikeuden mukaan sitovia. Tämän säännön asema ja voimaantulopäivä on hyvä tarkastaa UNECE:n asiakirjan TRANS/WP.29/343 viimeisimmästä versiosta. Asiakirja saatavana osoitteessa https://unece.org/status-1958-agreement-and-annexed-regulations

E-sääntö nro 155 – Yhdenmukaiset vaatimukset, jotka koskevat ajoneuvojen hyväksyntää kyberturvallisuuden ja sen hallintajärjestelmän osalta [2025/5]

Sisältää kaiken voimassa olevan tekstin seuraaviin asti:

Täydennys 3 säännön alkuperäiseen versioon – Voimaantulopäivä: 10. tammikuuta 2025

Tämä asiakirja on ainoastaan dokumentointitarkoituksiin. Todistusvoimaiset, oikeudellisesti sitovat tekstit ovat seuraavat:

— ECE/TRANS/WP.29/2020/79 (sellaisena kuin se on muutettuna asiakirjoilla ECE/TRANS/WP.29/2020/94 ja ECE/TRANS/WP.29/2020/97)

— ECE/TRANS/WP.29/2022/54

— ECE/TRANS/WP.29/2023/70 ja

— ECE/TRANS/WP.29/2024/55

SISÄLLYSLUETTELO

Sääntö

1. Soveltamisala
2. Määritelmät
3. Hyväksynnän hakeminen
4. Merkinnät
5. Hyväksyntä
6. Kyberturvallisuuden hallintajärjestelmän vaatimustenmukaisuustodistus
7. Vaatimukset
8. Ajoneuvotyypin muutokset ja tyyppihyväksynnän laajentaminen
9. Tuotannon vaatimustenmukaisuus
10. Seuraamukset vaatimustenmukaisuudesta poikkeavasta tuotannosta
11. Tuotannon lopettaminen
12. Hyväksyntätesteistä vastaavien tutkimuslaitosten ja tyyppihyväksyntäviranomaisten nimet ja osoitteet

Liitteet

1 Ilmoituslomake

2 Ilmoitus

3 Hyväksyntämerkki

4 Kyberturvallisuuden hallintajärjestelmän vaatimustenmukaisuustodistuksen malli

5 Luettelo uhkista ja niiden lieventämiseksi toteutetuista toimista

1. Soveltamisala

1.1. Tätä sääntöä sovelletaan kyberturvallisuuden osalta luokkien L, M, N ja O ajoneuvoihin, joissa on ainakin yksi elektroninen ohjausyksikkö.

1.2. Tämä sääntö ei rajoita sellaisten muiden E-sääntöjen taikka alueellisten tai kansallisten säädösten soveltamista, joilla säännellään valtuutettujen tahojen pääsyä käsiksi ajoneuvoon taikka sen tietoihin, toimintoihin ja resursseihin sekä tällaisen pääsyluvan edellytyksiä. Se ei rajoita myöskään sellaisten kansallisten tai alueellisten säädösten soveltamista, jotka liittyvät yksityisyyden suojaan ja luonnollisten henkilöiden suojeluun heidän henkilötietojensa käsittelyssä.

1.3. Tämä sääntö ei rajoita sellaisten muiden E-sääntöjen taikka alueellisten tai kansallisten säädösten soveltamista, joilla säännellään fyysisten ja digitaalisten varaosien ja korvaavien komponenttien kehittämistä ja asentamista tai järjestelmään integroimista kyberturvallisuuden osalta.

2. Määritelmät

Tässä säännössä sovelletaan seuraavia määritelmiä:

2.1. '*Ajoneuvotyypillä*' tarkoitetaan ajoneuvoja, jotka eivät eroa toisistaan ainakaan seuraavilta olennaisilta ominaisuuksiltaan:

a) valmistajan ajoneuvotyypille antama nimitys

b) sähköisen/elektronisen arkkitehtuurin ja ulkoisten liitäntöjen olennaiset ominaisuudet kyberturvallisuuden kannalta.

2.2. '*Kyberturvallisuudella*' tarkoitetaan maantieajoneuvojen ja niiden toimintojen suojaamista sähköisiin tai elektronisiin komponentteihin kohdistuvilta kyberuhkilta.

2.3. '*Kyberturvallisuuden hallintajärjestelmällä (CSMS)* tarkoitetaan riskiperusteista järjestelyä, jolla määritellään ne organisatoriset prosessit, vastuut ja hallinnolliset toimet, joilla puututaan ajoneuvoihin kohdistuviin kyberuhkiin ja suojataan ajoneuvoja kyberhyökkäyksiltä.

2.4. '*Järjestelmällä*' tarkoitetaan komponenttien ja/tai osajärjestelmien kokoonpanoa, jolla toteutetaan toiminto tai toimintoja.

2.5. '*Kehittämisvaiheella*' tarkoitetaan ajoneuvotyypin tyyppihyväksyntää edeltävää vaihetta.

2.6. '*Tuotantovaiheella*' tarkoitetaan ajoneuvotyypin tuotannon kestoaikaa.

2.7. '*Tuotannon jälkeisellä vaiheella*' tarkoitetaan aikaa ajoneuvotyypin tuotannon lopettamisesta kaikkien ajoneuvotyyppiin kuuluvien ajoneuvojen käyttöajan päättymiseen. Tietyn ajoneuvotyypin muodostavia ajoneuvoja on tämän vaiheen aikana käytössä, mutta niitä ei enää valmisteta. Vaihe päättyy, kun ajoneuvotyyppiin kuuluvia ajoneuvoja ei enää ole käytössä.

2.8. '*Lieventämistoimenpiteellä*' tarkoitetaan toimenpidettä, joka pienentää riskiä.

2.9. '*Riskillä*' tarkoitetaan mahdollisuutta, että tietty uhka hyödyntää ajoneuvon haavoittuvuuksia ja aiheuttaa tällä tavoin vahinkoa asianomaiselle organisaatiolle tai henkilölle.

2.10. '*Riskinarvioinnilla*' tarkoitetaan riskin havaitsemisen, tunnustamisen ja kuvaamisen käsittävää prosessia (riskin tunnistaminen), jolla pyritään saamaan käsitys riskin luonteesta ja määrittämään sen taso (riskianalyysi) ja jossa vertaillaan riskianalyysin tuloksia riskikriteereihin sen määrittämiseksi, onko riski ja/tai sen suuruus hyväksyttävä tai siedettävä (riskinarviointi).

2.11. '*Riskinhallinnalla*' tarkoitetaan koordinoituja toimia, joilla ohjataan ja valvotaan organisaatiota riskin osalta.

2.12. '*Uhkalla*' tarkoitetaan mahdollista syytä ei-toivottuun tapahtumaan, joka voi aiheuttaa vahinkoa järjestelmälle, organisaatiolle tai yksilölle.

2.13. '*Haavoittuvuudella*' tarkoitetaan omaisuuserän tai lieventämistoimenpiteen heikkoutta, jota yksi tai useampi uhka voi hyödyntää.

3. Hyväksynnän hakeminen

3.1. Hakemuksen ajoneuvotyypin hyväksymiseksi kyberturvallisuuden osalta tekee ajoneuvon valmistaja tai tämän asianmukaisesti valtuutettu edustaja.

3.2. Hakemukseen on liitettävä jäljempänä mainitut asiakirjat kolmena kappaleena sekä seuraavat tiedot:

3.2.1. Ajoneuvotyypin kuvaus tämän säännön liitteessä 1 mainittujen seikkojen osalta.

3.2.2. Jos näiden tietojen on osoitettu kuuluvan teollis- ja tekijänoikeuksien piiriin tai edustavan valmistajan tai tämän toimittajien erityistä taitotietoa, valmistajan tai tämän toimittajien on annettava riittävät tiedot, joiden perusteella tässä säännössä tarkoitetut tarkastukset voidaan tehdä asianmukaisesti. Tällaisia tietoja käsitellään luottamuksellisina.

3.2.3. Tämän säännön kohdan 6 mukainen kyberturvallisuuden hallintajärjestelmän vaatimustenmukaisuustodistus.

3.3. Asiakirja-aineisto koostuu seuraavista kahdesta osasta:

a) Hyväksyntää varten tarvittava virallinen asiakirjapaketti, joka sisältää liitteessä 1 eritellyn aineiston ja joka on toimitettava hyväksyntäviranomaiselle tai sen tutkimuslaitokselle tyyppihyväksyntähakemuksen yhteydessä. Hyväksyntäviranomainen tai tutkimuslaitos käyttää pakettia perusvertailuaineistona hyväksyntämenettelyssä. Hyväksyntäviranomaisen tai tutkimuslaitoksen on varmistettava, että asiakirjapaketti pidetään saatavilla vähintään kymmenen vuotta siitä, kun ajoneuvon tuotanto on lopetettu kokonaan.

b) Valmistaja voi pitää hallussaan muuta aineistoa, jolla on merkitystä tämän säännön vaatimusten kannalta. Aineisto on asetettava saataville tyyppihyväksynnän yhteydessä. Valmistajan on varmistettava, että tyyppihyväksynnän yhteydessä saataville asetettu aineisto on saatavilla kymmenen vuoden ajan siitä, kun ajoneuvon tuotanto on lopetettu kokonaan.

4. Merkinnät

4.1. Jokaiseen tämän säännön mukaisesti hyväksyttyä ajoneuvotyyppiä vastaavaan ajoneuvoon on kiinnitettävä näkyvästi hyväksyntälomakkeessa määriteltyyn helppopääsyiseen paikkaan kansainvälinen hyväksyntämerkki, joka koostuu seuraavista:

4.1.1. E-kirjain ja hyväksynnän myöntäneen maan tunnusnumero, jotka ovat ympyrän sisällä

4.1.2. kohdassa 4.1.1 tarkoitetun ympyrän oikealla puolella sijaitseva tämän säännön numero, jota seuraa R-kirjain, viiva ja tyyppihyväksyntänumero.

4.2. Kohdassa 4.1.1 määriteltyä tunnusta ei tarvitse toistaa, jos ajoneuvo vastaa ajoneuvotyyppiä, joka on hyväksytty yhden tai useamman sopimukseen liitetyn muun säännön mukaisesti maassa, joka on myöntänyt hyväksynnän tämän säännön mukaisesti. Tällaisessa tapauksessa kaikkien niiden sääntöjen numerot, hyväksyntänumerot ja lisätunnukset, joiden mukaisesti hyväksyntä on myönnetty hyväksynnän tämän säännön mukaisesti myöntäneessä maassa, on merkittävä pystysarakkeisiin kohdassa 4.1.1 määritellyn tunnuksen oikealle puolelle.

4.3. Hyväksyntämerkin on oltava helposti luettavissa ja pysyvä.

4.4. Hyväksyntämerkki on sijoitettava valmistajan kiinnittämään ajoneuvon tyyppikilpeen tai sen lähelle.

4.5. Tämän säännön liitteessä 3 annetaan esimerkkejä hyväksyntämerkeistä.

5. Hyväksyntä

5.1. Hyväksyntäviranomaiset myöntävät tyyppihyväksynnän kyberturvallisuuden osalta ainoastaan sellaisille ajoneuvotyypeille, jotka täyttävät tämän säännön vaatimukset.

5.1.1. Hyväksyntäviranomaisen tai tutkimuslaitoksen on asiakirjatarkastuksin todennettava, että ajoneuvonvalmistaja on toteuttanut ajoneuvotyypin osalta toimenpiteet, joilla huolehditaan seuraavista:

a) Tässä säännössä vaaditut tiedot kerätään ja todennetaan koko toimitusketjusta sen osoittamiseksi, että toimittajiin liittyvät riskit on tunnistettu ja hallitaan.

b) Ajoneuvotyyppiä koskeva riskinarviointi (kehittämisvaiheessa tai jälkikäteen), testaustulokset ja sovelletut lieventämistoimenpiteet dokumentoidaan, myös riskinarviointia tukevat suunnittelutiedot.

c) Ajoneuvotyypin suunnittelussa toteutetaan asianmukaiset kyberturvallisuustoimenpiteet.

d) Mahdolliset kyberturvallisuushyökkäykset havaitaan ja niihin reagoidaan.

e) Pidetään kirjaa tiedoista kyberhyökkäyksien havaitsemisen tueksi ja huolehditaan siitä, että käytettävissä on tietojenkäsittelyvalmiudet kyberhyökkäysyritysten tai onnistuneiden kyberhyökkäysten analysoimiseksi.

5.1.2. Hyväksyntäviranomaisen tai tutkimuslaitoksen on ajoneuvotyyppiä edustavalle ajoneuvolle tehtävillä testeillä todennettava, että ajoneuvonvalmistaja on toteuttanut dokumentoimansa kyberturvallisuustoimenpiteet. Nämä otantaan perustuvat testit tekee hyväksyntäviranomainen tai tutkimuslaitos joko itse tai yhteistyössä ajoneuvonvalmistajan kanssa. Otannassa on keskityttävä erityisesti mutta ei pelkästään riskeihin, jotka on riskinarvioinnissa arvioitu suuriksi.

5.1.3. Hyväksyntäviranomaisen tai tutkimuslaitoksen on evättävä tyyppihyväksyntä kyberturvallisuuden osalta, jos ajoneuvonvalmistaja ei ole täyttänyt kohdassa 7.3 tarkoitetuista vaatimuksista yhtä tai useampaa ja erityisesti seuraavia:

a) Ajoneuvonvalmistaja ei ole tehnyt kohdassa 7.3.3 tarkoitettua kattavaa riskinarviointia eli ei esimerkiksi ole tarkastellut kaikkia liitteen 5 osassa A tarkoitettuihin uhkiin liittyviä riskejä.

b) Ajoneuvonvalmistaja ei ole suojannut ajoneuvotyyppiä riskinarvioinnissaan yksilöidyiltä riskeiltä, tai kohdassa 7 edellytettyjä oikeasuhteisia lieventämistoimenpiteitä ei ole toteutettu.

c) Ajoneuvonvalmistaja ei ole toteuttanut asianmukaisia ja oikeasuhteisia toimenpiteitä, joilla suojataan ajoneuvotyypissä (mahdollisesti) olevat ympäristöt, jotka on tarkoitettu jälkimarkkinoiden ohjelmistojen, palvelujen, sovellusten tai datan tallentamista ja käyttöä varten.

d) Ajoneuvonvalmistaja ei ole ennen hyväksyntää tehnyt asianmukaisia ja riittäviä testejä, joilla todennetaan toteutettujen turvatoimien tehokkuus.

5.1.4. Arvioivan hyväksyntäviranomaisen on evättävä tyyppihyväksyntä kyberturvallisuuden osalta myös siinä tapauksessa, että hyväksyntäviranomainen tai tutkimuslaitos ei ole saanut ajoneuvonvalmistajalta riittäviä tietoja ajoneuvotyypin kyberturvallisuuden arvioimiseksi.

5.2. Tätä sääntöä soveltaville vuoden 1958 sopimuksen sopimuspuolille on ilmoitettava tähän sääntöön perustuvasta ajoneuvotyypin hyväksynnästä tai hyväksynnän laajentamisesta tai epäämisestä tämän säännön liitteessä 2 esitetyn mallin mukaisella lomakkeella.

5.3. Hyväksyntäviranomaiset eivät saa myöntää tyyppihyväksyntää varmistamatta, että valmistaja on ottanut käyttöön tyydyttävät järjestelyt ja menettelyt tämän säännön kattamien kyberturvallisuusnäkökohtien asianmukaista hallintaa varten.

5.3.1. Hyväksyntäviranomaisen ja sen tutkimuslaitosten on varmistettava vuoden 1958 sopimuksen liitteessä 2 vahvistettujen kriteerien täyttymisen lisäksi seuraavat:

a) Niillä on pätevät työntekijät, joilla on asianmukaiset kyberturvallisuustaidot ja erityisesti autoihin liittyvien riskien arviointiin tarvittava osaaminen. ([1])

b) Niillä on käytössä menettelyt tämän säännön mukaista yhdenmukaista arviointia varten.

5.3.2. Tätä E-sääntöä soveltavan sopimuspuolen on hyväksyntäviranomaisensa välityksellä ilmoitettava ja annettava tiedoksi muiden tätä E-sääntöä soveltavien sopimuspuolten hyväksyntäviranomaisille ne menetelmät ja perusteet, joiden mukaisesti ilmoittava viranomainen arvioi tämän säännön ja etenkin sen kohtien 5.1, 7.2 ja 7.3 mukaisesti toteutettujen toimenpiteiden asianmukaisuuden.

Nämä tiedot on toimitettava a) ennen ensimmäisen tämän säännön mukaisen hyväksynnän myöntämistä ja b) aina kun arviointimenetelmää tai -perusteita päivitetään.

Tietojen toimittamisen tarkoituksena on mahdollistaa parhaiden käytäntöjen kerääminen ja analysointi ja varmistaa, että kaikki tätä sääntöä soveltavat hyväksyntäviranomaiset soveltavat sitä yhdenmukaisesti.

5.3.3. Kohdassa 5.3.2 tarkoitetut tiedot on ladattava englanninkielisinä Yhdistyneiden kansakuntien Euroopan talouskomission perustamaan DETA-tietokantaan ([2]) ripeästi ja viimeistään 14 päivää ennen kuin ensimmäistä kertaa myönnetään hyväksyntä asianomaisten arviointimenetelmien ja -perusteiden mukaisesti. Tietojen perusteella on voitava saada selko niistä vähimmäissuoritustasoista, joita hyväksyntäviranomainen soveltaa kuhunkin kohdassa 5.3.2 tarkoitettuun vaatimukseen, ja niistä menettelyistä ja toimenpiteistä, joilla se varmentaa, että nämä vähimmäissuoritustasot täyttyvät. ([3])

5.3.4. Kun hyväksyntäviranomaiset ovat saaneet kohdassa 5.3.2 tarkoitetut tiedot, ne voivat esittää ilmoittavalle hyväksyntäviranomaiselle huomautuksia lataamalla ne DETA-tietokantaan 14 päivän kuluessa tiedoksiantopäivästä.

5.3.5. Jos hyväksynnän myöntävä hyväksyntäviranomainen ei voi ottaa kohdan 5.3.4 mukaisesti saatuja huomautuksia huomioon, huomautuksia lähettäneiden hyväksyntäviranomaisten ja hyväksynnän myöntävän hyväksyntäviranomaisen on haettava asiaan lisäselvityksiä vuoden 1958 sopimuksen liitteen 6 mukaisesti. Ajoneuvoja koskevien sääntöjen yhdenmukaistamista käsittelevän maailmanfoorumin (WP.29) asianomainen tätä sääntöä tarkasteleva työryhmä ([4]) sopii arviointimenetelmien ja -perusteiden yhteisestä tulkinnasta. ([5]) Tätä yhteistä tulkintaa on sovellettava yhteisesti, ja kaikkien hyväksyntäviranomaisten on myönnettävä tähän sääntöön perustuvat tyyppihyväksynnät sen mukaisesti.

([1]) Esim. standardit ISO 26262-2018, ISO/PAS 21448 ja ISO/SAE 21434.
([2]) https://www.unece.org/trans/main/wp29/datasharing.html.
([3]) Ladattavista yksityiskohtaisista tiedoista (esim. menetelmä, kriteerit, suoritustaso) ja niiden esittämismuodosta annetaan ohjeita tulkinta-asiakirjassa, jonka kyberturvallisuutta ja langatonta viestintää käsittelevä työryhmä laatii esitettäväksi GRVA-työryhmän seitsemännessä kokouksessa.
([4]) Automatisoituja/autonomisia ja verkkoon liitettyjä ajoneuvoja käsittelevä työryhmä (GRVA).
([5]) Tulkinta on otettava huomioon kohdan 5.3.3 alaviitteessä tarkoitetussa tulkinta-asiakirjassa.

5.3.6. Kaikkien hyväksyntäviranomaisten, jotka myöntävät tyyppihyväksynnän tämän säännön mukaisesti, on ilmoitettava myöntämästään hyväksynnästä muille hyväksyntäviranomaisille. Hyväksyntäviranomaisen on ladattava tyyppihyväksyntä ja sitä täydentävät asiakirjat englanninkielisinä DETA-tietokantaan 14 päivän kuluessa hyväksynnän myöntämisestä. ([6])

5.3.7. Sopimuspuolet voivat tarkastella kohdan 5.3.6 mukaisesti tallennettujen tietojen perusteella myönnettyjä hyväksyntiä. Sopimuspuolten mahdolliset näkemyserot ratkaistaan vuoden 1958 sopimuksen 10 artiklan ja liitteen 6 mukaisesti. Sopimuspuolten on ilmoitettava vuoden 1958 sopimuksen liitteessä 6 tarkoitetuista tulkintaeroistaan myös ajoneuvoja koskevien sääntöjen yhdenmukaistamista käsittelevän maailmanfoorumin (WP.29) asianomaiselle työryhmälle. Työryhmä auttaa näkemyserojen ratkaisemisessa ja kuulee asiasta tarvittaessa WP.29:ää.

5.4. Tämän säännön kohdan 7.2 soveltamiseksi valmistajan on varmistettava, että tämän säännön soveltamisalaan kuuluvat kyberturvallisuusnäkökohdat pannaan täytäntöön.

6. Kyberturvallisuuden hallintajärjestelmän vaatimustenmukaisuustodistus

6.1. Sopimuspuolten on nimettävä hyväksyntäviranomainen, joka suorittaa valmistajan arvioinnin ja antaa kyberturvallisuuden hallintajärjestelmän vaatimustenmukaisuustodistuksen.

6.2. Kyberturvallisuuden hallintajärjestelmän vaatimustenmukaisuustodistusta koskevan hakemuksen tekee ajoneuvonvalmistaja tai tämän asianmukaisesti valtuutettu edustaja.

6.3. Hakemukseen on liitettävä jäljempänä mainitut asiakirjat kolmena kappaleena sekä seuraavat tiedot:

6.3.1. kyberturvallisuuden hallintajärjestelmän kuvaus

6.3.2. allekirjoitettu vakuutus, joka vastaa liitteen 1 lisäyksessä 1 esitettyä mallia.

6.4. Arvioinnin yhteydessä valmistajan on liitteen 1 lisäyksessä 1 esitettyä mallia käyttäen vakuutettava ja tyyppihyväksyntäviranomaista tai sen tutkimuslaitosta tyydyttävällä tavalla osoitettava, että sillä on käytössä menettelyt, joita tarvitaan kaikkien tämän säännön mukaisten kyberturvallisuusvaatimusten noudattamiseen.

6.5. Kun arviointi on saatu hyväksyttävästi päätökseen ja valmistajalta on saatu liitteen 1 lisäyksessä 1 esitetyn mallin mukainen allekirjoitettu vakuutus, valmistajalle annetaan tämän säännön liitteessä 4 kuvattu kyberturvallisuuden hallintajärjestelmän vaatimustenmukaisuustodistus.

6.6. Hyväksyntäviranomaisen tai sen tutkimuslaitoksen on laadittava kyberturvallisuuden hallintajärjestelmän vaatimustenmukaisuustodistus tämän säännön liitteessä 4 esitetyn mallin mukaisesti.

6.7. Kyberturvallisuuden hallintajärjestelmän vaatimustenmukaisuustodistus on voimassa enintään kolme vuotta todistuksen antamispäivästä, ellei sitä peruuteta.

6.8. Kyberturvallisuuden hallintajärjestelmän vaatimustenmukaisuustodistuksen myöntänyt hyväksyntäviranomainen voi milloin tahansa varmentaa, että sitä koskevat vaatimukset täyttyvät edelleen. Hyväksyntäviranomaisen on peruutettava kyberturvallisuuden hallintajärjestelmän vaatimustenmukaisuustodistus, jos tässä säännössä vahvistetut vaatimukset eivät enää täyty.

([6]) GRVA-työryhmä laatii tarkempia ohjeita asiakirjapakettiin liittyvistä vähimmäisvaatimuksista seitsemännen kokouksensa aikana.

6.9. Valmistajan on ilmoitettava hyväksyntäviranomaiselle tai sen tutkimuslaitokselle kaikista muutoksista, jotka vaikuttavat kyberturvallisuuden hallintajärjestelmän vaatimustenmukaisuustodistuksen pätevyyteen. Hyväksyntäviranomainen tai sen tutkimuslaitos päättää valmistajaa kuultuaan, tarvitaanko uusia tarkastuksia.

6.10. Jotta hyväksyntäviranomainen voi saattaa arviointinsa päätökseen ennen kyberturvallisuuden hallintajärjestelmän vaatimustenmukaisuustodistuksen voimassaolon päättymistä, valmistajan on hyvissä ajoin haettava uutta todistusta tai todistuksen voimassaolon jatkamista. Jos arvio on myönteinen, hyväksyntäviranomaisen on annettava uusi kyberturvallisuuden hallintajärjestelmän vaatimustenmukaisuustodistus tai jatkettava todistuksen voimassaoloa kolmella vuodella. Hyväksyntäviranomaisen on varmennettava, että kyberturvallisuuden hallintajärjestelmä on edelleen tämän säännön vaatimusten mukainen. Hyväksyntäviranomaisen on annettava uusi todistus, jos muutokset on tuotu sen tai sen tutkimuslaitoksen tietoon ja niistä on tehty myönteinen arviointi.

6.11. Valmistajalle myönnetyn kyberturvallisuuden hallintajärjestelmän vaatimustenmukaisuustodistuksen voimassaolon päättymistä tai peruuttamista on niiden ajoneuvotyyppien osalta, joihin hallintajärjestelmä on tarkoitettu, pidettävä kohdassa 8 tarkoitettuna hyväksynnän muutoksena, joka voi johtaa hyväksynnän peruuttamiseen, jos sen myöntämisen edellytykset eivät enää täyty.

7. Vaatimukset

7.1. Yleiset vaatimukset

7.1.1. Tämän säännön vaatimukset eivät rajoita muiden E-sääntöjen määräysten tai vaatimusten soveltamista.

7.2. Kyberturvallisuuden hallintajärjestelmää koskevat vaatimukset

7.2.1. Arviointia varten hyväksyntäviranomaisen tai sen tutkimuslaitoksen on varmennettava, että ajoneuvonvalmistajalla on käytössä kyberturvallisuuden hallintajärjestelmä ja että se on tämän säännön mukainen.

7.2.2. Kyberturvallisuuden hallintajärjestelmän on katettava seuraavat seikat:

7.2.2.1. Ajoneuvonvalmistajan on osoitettava hyväksyntäviranomaiselle tai tutkimuslaitokselle, että sen kyberturvallisuuden hallintajärjestelmää sovelletaan seuraaviin vaiheisiin:

a) kehittämisvaihe

b) tuotantovaihe

c) tuotannon jälkeinen vaihe.

7.2.2.2. Ajoneuvonvalmistajan on osoitettava, että sen kyberturvallisuuden hallintajärjestelmässä käytettävillä menettelyillä varmistetaan, että turvallisuusseikat, kuten liitteessä 5 luetellut riskit ja riskienlieventämistoimenpiteet, otetaan asianmukaisesti huomioon. Menettelyitä ovat

a) menettelyt, joita valmistajan organisaatiossa käytetään kyberturvallisuuden hallintaan

b) menettelyt, joilla kartoitetaan ajoneuvotyyppeihin kohdistuvat riskit ja joiden yhteydessä tarkastellaan liitteen 5 osassa A mainittuja ja muita asiaan liittyviä riskejä

c) menettelyt, joita käytetään kartoitettujen riskien arviointiin, luokitteluun ja käsittelyyn

d) menettelyt, joilla varmennetaan, että kartoitettujen riskien hallinta on asianmukaista

e) menettelyt, joilla testataan ajoneuvotyypin kyberturvallisuus

f) menettelyt, joilla varmistetaan, että riskinarviointi pidetään ajan tasalla

g) menettelyt, joilla harjoitetaan seurantaa ajoneuvotyyppeihin liittyvien kyberhyökkäysten, kyberuhkien ja haavoittuvuuksien varalta, havaitaan ne ja reagoidaan niihin, sekä menettelyt, joilla arvioidaan, ovatko toteutetut kyberturvallisuustoimenpiteet havaittujen uusien kyberuhkien ja haavoittuvuuksien valossa edelleen tehokkaita

h) menettelyt, joilla tuotetaan merkityksellistä tietoa kyberhyökkäysyritysten tai onnistuneiden kyberhyökkäysten analysoinnin tueksi.

7.2.2.3. Ajoneuvonvalmistajan on osoitettava, että sen kyberturvallisuuden hallintajärjestelmässä käytettävillä menettelyillä varmistetaan, että kohdan 7.2.2.2 alakohdissa c ja g tarkoitettuun luokitteluun perustuvien kyberuhkien ja haavoittuvuuksien, jotka edellyttävät ajoneuvonvalmistajan toimia, lieventämiseksi toteutetaan toimenpiteitä kohtuullisessa ajassa.

7.2.2.4. Ajoneuvonvalmistajan on osoitettava, että sen kyberturvallisuuden hallintajärjestelmässä käytettävillä menettelyillä varmistetaan, että kohdan 7.2.2.2 alakohdassa g tarkoitettu seuranta on jatkuvaa. Seurannan on

a) käynnistyttävä ajoneuvon ensirekisteröinnistä

b) mahdollistettava kyberuhkien, haavoittuvuuksien ja kyberhyökkäysten analysointi ja havaitseminen ajoneuvon tietojen ja lokitiedostojen avulla. Tämän mahdollisuuden käytössä on noudatettava kohtaa 1.3 ja kunnioitettava autonomistajien tai kuljettajien yksityisyyttä etenkin tietojen käyttöön annettavan suostumuksen osalta.

7.2.2.5. Ajoneuvonvalmistajan on osoitettava, kuinka sen kyberturvallisuuden hallintajärjestelmällä hallitaan sellaisia kohdan 7.2.2.2 vaatimuksiin liittyviä tekijöitä, joiden osalta se voi olla riippuvainen tavarantoimittajistaan, palveluntarjoajistaan tai alaorganisaatioistaan.

7.3. Ajoneuvotyyppejä koskevat vaatimukset

7.3.1. Valmistajalla on oltava hyväksyttävää ajoneuvotyyppiä koskeva voimassa oleva kyberturvallisuuden hallintajärjestelmän vaatimustenmukaisuustodistus. Kun kyse on luokkien M, N ja O ajoneuvoille ennen 1. heinäkuuta 2024 tai luokan L ajoneuvoille ennen 1. heinäkuuta 2029 myönnetyistä ensimmäisistä tyyppihyväksynnistä ja niiden laajennuksista, joiden tapauksessa ajoneuvonvalmistaja voi osoittaa, että ajoneuvotyyppiä ei ole voitu kehittää kyberturvallisuuden hallintajärjestelmän mukaisesti, ajoneuvonvalmistajan on kuitenkin osoitettava, että kyberturvallisuus on otettu asianmukaisesti huomioon kyseisen ajoneuvotyypin kehittämisvaiheessa.

7.3.2. Ajoneuvonvalmistajan on kartoitettava ja hallittava hyväksyttävää ajoneuvotyyppiä koskevat toimittajiin liittyvät riskit.

7.3.3. Ajoneuvonvalmistajan on kartoitettava ajoneuvotyyppiin liittyvät kriittiset elementit ja tehtävä ajoneuvotyypille kattava riskinarviointi sekä huolehdittava siitä, että havaittuihin riskeihin puututaan tai ne hallitaan asianmukaisesti. Riskinarvioinnissa on tarkasteltava ajoneuvotyypin yksittäisiä elementtejä ja niiden vuorovaikutusta. Riskinarvioinnissa on lisäksi tarkasteltava vuorovaikutusta mahdollisten ulkoisten järjestelmien kanssa. Riskejä arvioidessaan ajoneuvonvalmistajan on tarkasteltava kaikkiin liitteen 5 osassa A tarkoitettuihin uhkiin liittyviä ja muita merkityksellisiä riskejä.

7.3.4. Ajoneuvonvalmistajan on suojattava ajoneuvotyyppi suorittamassaan riskinarvioinnissa kartoitetuilta riskeiltä. Ajoneuvotyypin suojaamiseksi on toteutettava oikeasuhteisia lieventämistoimenpiteitä. Lieventämistoimenpiteisiin on sisällyttävä kaikki liitteen 5 osissa B ja C tarkoitetut toimenpiteet, jotka ovat kartoitettujen riskien kannalta merkityksellisiä. Jos jokin liitteen 5 osassa B tai C tarkoitettu lieventämistoimenpide ei ole riskin kannalta merkityksellinen tai riittävä, ajoneuvonvalmistajan on huolehdittava siitä, että toteutetaan jokin toinen asianmukainen lieventämistoimenpide.

Etenkin kun kyse on luokkien M, N ja O ajoneuvoille ennen 1. heinäkuuta 2024 tai luokan L ajoneuvoille ennen 1. heinäkuuta 2029 myönnetyistä ensimmäisistä tyyppihyväksynnistä ja niiden laajennuksista, ajoneuvonvalmistajan on huolehdittava siitä, että jos liitteen 5 osassa B tai C tarkoitettu lieventämistoimenpide ei ole teknisesti toteutettavissa, toteutetaan jokin toinen asianmukainen lieventämistoimenpide. Valmistajan on toimitettava hyväksyntäviranomaiselle teknisestä toteutettavuudesta tehty arviointi.

7.3.5. Ajoneuvonvalmistajan on toteutettava asianmukaiset ja oikeasuhteiset toimenpiteet, joilla suojataan ajoneuvotyypissä (mahdollisesti) olevat ympäristöt, jotka on tarkoitettu jälkimarkkinoiden ohjelmistojen, palvelujen, sovellusten tai tietojen tallentamista ja käyttöä varten.

7.3.6. Ajoneuvonvalmistajan on ennen tyyppihyväksyntää tehtävä asianmukaiset ja riittävät testit, joilla todennetaan toteutettujen turvatoimien tehokkuus.

7.3.7. Ajoneuvonvalmistajan on toteutettava ajoneuvotyypin osalta toimenpiteet, joilla

a) havaitaan ja estetään kyseiseen ajoneuvotyyppiin kuuluviin ajoneuvoihin kohdistuvat kyberhyökkäykset

b) tuetaan ajoneuvonvalmistajan seurantavalmiuksia, jotka koskevat ajoneuvotyyppiin liittyviä uhkia, haavoittuvuuksia ja kyberhyökkäyksiä

c) luodaan tietojenkäsittelyvalmiudet kyberhyökkäysyritysten tai onnistuneiden kyberhyökkäysten analysoimiseksi.

7.3.8. Tämän säännön soveltamiseksi käytettävien salausmoduulien on oltava yhdenmukaisten standardien mukaisia. Jos käytetyt salausmoduulit eivät ole yhdenmukaisten standardien mukaisia, ajoneuvonvalmistajan on perusteltava niiden käyttö.

7.4. Raportointimääräykset

7.4.1. Ajoneuvonvalmistajan on vähintään kerran vuodessa ja tarvittaessa useamminkin ilmoitettava hyväksyntäviranomaiselle tai tutkimuslaitokselle kohdan 7.2.2.2 alakohdassa g tarkoitettujen seurantatoimiensa tulokset, mukaan luettuina merkitykselliset tiedot uusista kyberhyökkäyksistä. Ajoneuvonvalmistajan on lisäksi ilmoitettava ja vahvistettava hyväksyntäviranomaiselle tai tutkimuslaitokselle, että niiden ajoneuvotyyppiensä osalta toteuttamat kyberturvallisuusriskien lieventämistoimenpiteet ovat edelleen tehokkaita ja että mahdollisiin lisätoimiin on ryhdytty.

7.4.2. Hyväksyntäviranomaisen tai tutkimuslaitoksen on todennettava toimitetut tiedot ja tarvittaessa kehotettava ajoneuvonvalmistajaa korjaamaan havaitut puutteet.

Jos raportointi tai reagointi ei ole riittävää, hyväksyntäviranomainen voi päättää peruuttaa kyberturvallisuuden hallintajärjestelmän vaatimustenmukaisuustodistuksen kohdan 6.8 mukaisesti.

8. Ajoneuvotyypin muutokset ja tyyppihyväksynnän laajentaminen

8.1. Ajoneuvotyyppiin tehtävistä muutoksista, jotka vaikuttavat sen tekniseen suorituskykyyn kyberturvallisuuden ja/tai tässä säännössä vaadittujen asiakirjojen osalta, on ilmoitettava ajoneuvotyypin hyväksyneelle hyväksyntäviranomaiselle. Hyväksyntäviranomainen voi tällöin

8.1.1. joko katsoa, että muutokset ovat edelleen voimassa olevan tyyppihyväksynnän vaatimusten ja dokumentointiedellytysten mukaisia, tai

8.1.2. tehdä kohdan 5 mukaisen täydentävän vaikutustenarvioinnin ja tarvittaessa vaatia testien suorittamisesta vastaavalta tutkimuslaitokselta uuden testausselosteen.

8.1.3. Hyväksynnän laajentamisen tai epäämisen vahvistus, jossa eritellään muutokset, on annettava tiedoksi tämän säännön liitteessä 2 esitetyn mallin mukaisella ilmoituslomakkeella. Hyväksynnän laajentamisen myöntäneen hyväksyntäviranomaisen on annettava laajentamiselle sarjanumero ja ilmoitettava siitä muille tätä sääntöä soveltaville vuoden 1958 sopimuksen sopimuspuolille tämän säännön liitteessä 2 esitetyn mallin mukaisella ilmoituslomakkeella.

9. Tuotannon vaatimustenmukaisuus

9.1. Tuotannon vaatimustenmukaisuuden testausmenettelyjen on vastattava vuoden 1958 sopimuksen liitteessä 1 (E/ECE/TRANS/505/Rev.3) vahvistettuja menettelyjä, ja seuraavassa esitettyjen vaatimusten on täytyttävä.

9.1.1. Hyväksynnän haltijan on varmistettava, että tuotannon vaatimustenmukaisuuden testien tulokset kirjataan ja että liiteasiakirjat ovat saatavilla hyväksyntäviranomaisen tai sen tutkimuslaitoksen kanssa sovitun ajan. Tämä aika ei saa olla pitempi kuin 10 vuotta tuotannon lopettamisesta.

9.1.2. Tyyppihyväksynnän myöntänyt hyväksyntäviranomainen voi milloin tahansa tarkastaa kussakin tuotantolaitoksessa sovellettavat vaatimustenmukaisuuden valvontamenetelmät. Tällaisia tarkastuksia tehdään tavallisesti kerran kolmessa vuodessa.

10. Seuraamukset vaatimustenmukaisuudesta poikkeavasta tuotannosta

10.1. Ajoneuvotyypille tämän säännön mukaisesti myönnetty hyväksyntä voidaan peruuttaa, jos tässä säännössä vahvistetut vaatimukset eivät täyty tai jos näyteajoneuvot eivät täytä tämän säännön vaatimuksia.

10.2. Jos hyväksyntäviranomainen peruuttaa aiemmin myöntämänsä hyväksynnän, sen on viipymättä ilmoitettava asiasta muille tätä sääntöä soveltaville sopimuspuolille tämän säännön liitteessä 2 esitetyn mallin mukaisella ilmoituslomakkeella.

11. Tuotannon lopettaminen

11.1. Jos hyväksynnän haltija lopettaa kokonaan tämän säännön perusteella hyväksytyn ajoneuvotyypin valmistamisen, hyväksynnän haltijan on ilmoitettava tästä hyväksynnän myöntäneelle viranomaiselle. Saatuaan asianmukaisen ilmoituksen viranomaisen on ilmoitettava asiasta tätä sääntöä soveltaville muille sopimuspuolille hyväksyntälomakkeella, jonka loppuun on suuraakkosin lisätty allekirjoituksella ja päiväyksellä varustettu merkintä ”TUOTANTO LOPETETTU”.

12. Hyväksyntätesteistä vastaavien tutkimuslaitosten ja tyyppihyväksyntäviranomaisten nimet ja osoitteet

12.1. Tätä sääntöä soveltavien sopimuspuolten on ilmoitettava Yhdistyneiden kansakuntien sihteeristölle hyväksyntätestien suorittamisesta vastaavien tutkimuslaitosten sekä niiden tyyppihyväksyntäviranomaisten nimet ja osoitteet, jotka myöntävät hyväksynnät ja joille lomakkeet todistukseksi muissa maissa myönnetystä hyväksynnästä taikka hyväksynnän laajentamisesta, epäämisestä tai peruuttamisesta on toimitettava.

LIITE 1

Ilmoituslomake

Seuraavat tiedot on tarvittaessa toimitettava kolmena kappaleena, ja niihin on liitettävä sisällysluettelo. Mahdolliset piirustukset on toimitettava asianmukaisessa mittakaavassa ja riittävän yksityiskohtaisina A4-koossa tai siihen kokoon taitettuina. Mahdollisten valokuvien on oltava riittävän yksityiskohtaisia.

1. Merkki (valmistajan kauppanimi): .....

2. Tyyppi ja yleiset kaupalliset kuvaukset: .....

3. Tyypin tunniste, jos se on merkitty ajoneuvoon: .....

4. Merkinnän sijainti: .....

5. Ajoneuvoluokat: .....

6. Valmistajan / valmistajan edustajan nimi ja osoite: .....

7. Kokoonpanotehtaiden nimet ja osoitteet: .....

8. Edustavan ajoneuvon valokuvat ja/tai piirustukset: .....

9. Kyberturvallisuus

9.1. Ajoneuvotyypin yleiset rakenteelliset ominaisuudet, mukaan luettuina seuraavat:

a) ajoneuvon järjestelmät, jotka ovat ajoneuvotyypin kyberturvallisuuden kannalta merkityksellisiä

b) näiden järjestelmien komponentit, jotka ovat kyberturvallisuuden kannalta merkityksellisiä

c) näiden järjestelmien vuorovaikutus ajoneuvotyypin muiden järjestelmien ja ulkoisten liitäntöjen kanssa.

9.2. Ajoneuvotyyppiä kuvaava kaavio

9.3. Kyberturvallisuuden hallintajärjestelmän vaatimustenmukaisuustodistuksen numero: .....

9.4. Hyväksyttävää ajoneuvotyyppiä koskevat asiakirjat, joissa kuvataan riskinarvioinnin tulokset ja havaitut riskit: .....

9.5. Hyväksyttävää ajoneuvotyyppiä koskevat asiakirjat, joissa kuvataan lueteltuja järjestelmiä tai ajoneuvotyyppiä koskevat toteutetut lieventämistoimenpiteet ja se, miten niillä puututaan ilmoitettuihin riskeihin: .....

9.6. Hyväksyttävää ajoneuvotyyppiä koskevat asiakirjat, joissa kuvataan jälkimarkkinoiden ohjelmistoille, palveluille, sovelluksille tai tiedoille tarkoitettujen ympäristöjen suojaus: .....

9.7. Hyväksyttävää ajoneuvotyyppiä koskevat asiakirjat, joissa esitetään ajoneuvotyypin ja sen järjestelmien kyberturvallisuuden todentamiseksi tehdyt testit ja niiden tulokset: .....

9.8. Kuvaus toimitusketjun tarkastelusta kyberturvallisuuden kannalta: .....

Liite 1 – Lisäys 1

Kyberturvallisuuden hallintajärjestelmää koskevan valmistajan vaatimustenmukaisuusvakuutuksen malli

Valmistajan vakuutus kyberturvallisuuden hallintajärjestelmää koskevien vaatimusten noudattamisesta

Valmistajan nimi: .....

Valmistajan osoite:.....

..... (*valmistajan nimi*)

vakuuttaa, että E-säännön nro 155 kohdassa 7.2 vahvistettujen kyberturvallisuuden hallintajärjestelmää koskevien vaatimusten noudattamiseen tarvittavat menettelyt on otettu käyttöön ja pidetään käytössä.

Paikka: .....

Päiväys: .....

Allekirjoittajan nimi:.....

Allekirjoittajan asema:.....

(Valmistajan edustajan leima ja allekirjoitus)

LIITE 2

Ilmoitus

(Enimmäiskoko: A4 (210 × 297 mm))



Antaja: Viranomaisen nimi:
……
……
……

Aihe: hyväksynnän myöntäminen
Ajoneuvotyy- hyväksynnän laajentaminen
pin: ([2]) hyväksynnän peruuttaminen pp/kk/vvvv alkaen
hyväksynnän epääminen
tuotannon lopettaminen

E-säännön nro 155 mukaisesti.

Hyväksyntänumero: ……

Laajennuksen numero:……

Laajennuksen syy: ……

1. Merkki (valmistajan kauppanimi): ……

2. Tyyppi ja yleiset kaupalliset kuvaukset……

3. Tyypin tunniste, jos se on merkitty ajoneuvoon: ……

3.1. Merkinnän sijainti:……

4. Ajoneuvoluokat: ……

5. Valmistajan / valmistajan edustajan nimi ja osoite: ……

6. Kokoonpanotehtaiden nimet ja osoitteet:……

7. Kyberturvallisuuden hallintajärjestelmän vaatimustenmukaisuustodistuksen numero:……

8. Testien suorittamisesta vastaava tutkimuslaitos:……

9. Testausselosteen päiväys: ……

10. Testausselosteen numero:……

11. Huomautukset (jos on):……

12. Paikka: ……

([1]) Hyväksynnän myöntäneen/laajentaneen/evänneen/peruuttaneen maan tunnusnumero (ks. säännön hyväksyntämääräykset).
([2]) Tarpeeton viivataan yli.

13. Päiväys: .....

14. Allekirjoitus: .....

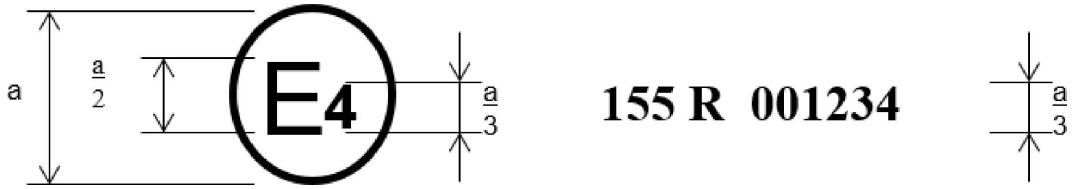
15. Liitteenä on luettelo hyväksyntäviranomaiselle luovutetusta aineistosta, joka on pyynnöstä saatavissa.

LIITE 3

Hyväksyntämerkki

MALLI A

(Ks. tämän säännön kohta 4.2)



a = vähintään 8 mm

Edellä olevasta ajoneuvoon kiinnitetystä hyväksyntämerkistä käy ilmi, että kyseinen maantiekäyttöön soveltuva ajoneuvotyyppi on hyväksytty Alankomaissa (E4) säännön nro 155 mukaisesti hyväksyntänumerolla 001234. Hyväksyntänumeron kaksi ensimmäistä merkkiä (00) tarkoittavat, että hyväksyntä on myönnetty tämän säännön vaatimusten mukaisesti säännön ollessa alkuperäisessä muodossaan.

LIITE 4

KYBERTURVALLISUUDEN HALLINTAJÄRJESTELMÄN VAATIMUSTENMUKAISUUSTODISTUKSEN MALLI

Todistus kyberturvallisuuden hallintajärjestelmän vaatimustenmukaisuudesta

suhteessa E-sääntöön nro 155

Todistuksen numero [*viitenumero*]

[..... *hyväksyntäviranomainen*]

todistaa, että

Valmistaja: .....

Valmistajan osoite: .....

noudattaa säännön nro 155 kohdan 7.2 määräyksiä

Tarkastukset on suorittanut (päiväys) .....

(hyväksyntäviranomaisen tai tutkimuslaitoksen nimi ja osoite): .....

Selosteen numero: .....

Tämä todistus on voimassa [..... *päivämäärä*] asti.

Tehty [..... *paikka*]

[..... *päiväys*]

[..... *Allekirjoitus*]

Liitteet: valmistajan antama kyberturvallisuuden hallintajärjestelmän kuvaus.

LIITE 5

Luettelo uhkista ja niiden lieventämiseksi toteutetuista toimista

1. Tässä liitteessä on kolme osaa. Liitteen osassa A annetaan peruskuvaus uhkista, haavoittuvuuksista ja hyökkäysmenetelmistä. Liitteen osassa B kuvataan ajoneuvotyyppeihin kohdistuvien uhkien lieventämistoimenpiteet. Osassa C kuvataan ajoneuvon ulkopuolelle (esim. tietoteknisiin taustaohjelmiin) kohdistuvien uhkien lieventämistoimenpiteet

2. Osat A, B ja C on otettava huomioon ajoneuvonvalmistajien toteuttamissa riskinarvioinneissa ja lieventämistoimenpiteissä.

3. Osassa A esitetään indeksoituina ylätason haavoittuvuudet ja niitä vastaavat esimerkit. Samaa indeksointia käytetään myös osien B ja C taulukoissa kunkin hyökkäyksen tai haavoittuvuuden yhdistämiseksi vastaaviin lieventämistoimenpiteisiin.

4. Uhka-analyysissä olisi otettava huomioon myös hyökkäyksen mahdolliset vaikutukset. Niistä voi olla apua riskin vakavuuden määrittämisessä ja lisäriskien tunnistamisessa. Hyökkäykset voivat

   a) vaarantaa ajoneuvon toimintaturvallisuuden

   b) keskeyttää ajoneuvon toimintoja

   c) muuttaa ohjelmistoja ja toimintakykyä

   d) muuttaa ohjelmistoja ilman vaikutuksia toimintaan

   e) rikkoa tietojen eheyden

   f) vaarantaa tietojen luottamuksellisuuden

   g) estää pääsyn tietoihin

   h) aiheuttaa muita vaikutuksia, myös luonteeltaan rikollisia.

OSA A

Uhkiin liittyvät haavoittuvuudet tai hyökkäysmenetelmät

Taulukossa A1 esitetään ylätason kuvaus uhkista ja niihin liittyvästä haavoittuvuudesta tai hyökkäysmenetelmistä.

Taulukko A1

Uhkiin liittyvät haavoittuvuudet tai hyökkäysmenetelmät

Ylä- ja alatason kuvaus haavoittuvuudesta/uhkasta			Esimerkki haavoittuvuudesta tai hyökkäysmenetelmästä	
4.3.1. Liikenteessä oleviin ajoneuvoihin liittyviä taustapalvelimia koskevat uhkat	1	Taustapalvelimien käyttö ajoneuvoon kohdistuviin hyökkäyksiin tai tietojen poimimiseen	1.1	Henkilöstö käyttää oikeuksiaan väärin (sisäpiirihyökkäys).
			1.2	Palvelimeen otetaan luvaton internetyhteys (esimerkiksi hyödyntämällä takaportteja, paikkaamattomia järjestelmäohjelmistojen haavoittuvuuksia, SQL-hyökkäyksiä tai muita keinoja).
			1.3	Palvelinta käytetään luvatta fyysisesti (esimerkiksi USB-muistitikulla tai muulla palvelimeen yhdistetyllä välineellä).
	2	Taustapalvelimen palvelujen häirintä, joka haittaa ajoneuvon toimintaa	2.1	Hyökkäys taustapalvelimeen pysäyttää sen toiminnan ja esimerkiksi estää sitä toimimasta vuorovaikutuksessa ajoneuvojen kanssa ja tarjoamaan niille niiden tarvitsemia palveluja.

Ylä- ja alatason kuvaus haavoittuvuudesta/uhkasta			Esimerkki haavoittuvuudesta tai hyökkäysmenetelmästä	
	3	Taustapalvelimilla säilytettävien ajoneuvoon liittyvien tietojen katoaminen tai vaarantuminen (”tietosuojaloukkaus”)	3.1	Henkilöstö käyttää oikeuksiaan väärin (sisäpiirihyökkäys).
			3.2	Pilvipalveluissa olevat tiedot katoavat. Hyökkäysten tai onnettomuuksien vuoksi voidaan menettää arkaluonteisia tietoja, joita säilytetään kolmannen osapuolen tarjoamissa pilvipalveluissa.
			3.3	Palvelimeen otetaan luvaton internetyhteys (esimerkiksi hyödyntämällä takaportteja, paikkaamattomia järjestelmäohjelmistojen haavoittuvuuksia, SQL-hyökkäyksiä tai muita keinoja).
			3.4	Palvelinta käytetään luvatta fyysisesti (esimerkiksi USB-muistitikulla tai muulla palvelimeen yhdistetyllä välineellä).
			3.5	Tietojen tahaton jakaminen vaarantaa tietosuojan (esim. hallinnolliset virheet).
4.3.2 Ajoneuvoihin niiden viestintäkanavien kautta kohdistuvat uhkat	4	Ajoneuvon vastaanottamien viestien tai tietojen väärentäminen	4.1	Viestejä väärennetään esiintymällä toisena henkilönä (esim. yhteistoiminnalliseen tietoisuuteen tai ajoliikkeiden koordinointiin käytettävät ajoneuvon ja toisen ajoneuvon tai muun tahon väliset V2X-viestit (CAM, MCM), GNSS-viestit jne.).
			4.2	Sybil-hyökkäys (muiden ajoneuvojen annetaan ymmärtää, että tiellä on useita ajoneuvoja)
	5	Viestintäkanavien käyttö ajoneuvossa säilytettävän koodin tai datan luvattomaan manipulointiin, poistamiseen tai muuhun muuttamiseen.	5.1	Viestintäkanavien kautta voidaan syöttää viestiliikenteeseen koodia, esimerkiksi muunneltua binaarikoodia.
			5.2	Viestintäkanavien kautta voidaan manipuloida ajoneuvossa säilytettävää koodia/dataa.
			5.3	Viestintäkanavien kautta voidaan korvata ajoneuvossa säilytettävää koodia/dataa.
			5.4	Viestintäkanavien kautta voidaan poistaa ajoneuvossa säilytettävää koodia/dataa.
			5.5	Viestintäkanavien kautta voidaan syöttää dataa/koodia ajoneuvoon (kirjoittaa dataa/koodia).
	6	Viestintäkanavat sallivat epäluotettavien viestien hyväksymisen tai ovat alttiita istuntojen kaappaamiselle tai toistohyökkäyksille.	6.1	Hyväksytään tietoja epäluotettavasta lähteestä.
			6.2	Väliintulohyökkäys / istunnon kaappaaminen.
			6.3	Toistohyökkäys: hyökkääjä voi esimerkiksi viestintäväylään kohdistetun hyökkäyksen avulla heikentää elektronisen ohjausyksikön ohjelmistoa tai väylässä käytettävää laiteohjelmistoa.
	7	Tietojen paljastuminen on helppoa. Voidaan esimerkiksi salakuunnella viestintää tai sallia luvaton pääsy arkaluonteisiin tiedostoihin tai kansioihin.	7.1	Tietojen sieppaaminen / häiritsevä säteily / viestinnän kuuntelu
			7.2	Hankitaan luvaton pääsy tiedostoihin tai tietoihin.

Ylä- ja alatason kuvaus haavoittuvuudesta/uhkasta			Esimerkki haavoittuvuudesta tai hyökkäysmenetelmästä	
	8	Ajoneuvon toimintojen häiritseminen viestintäkanavien kautta tehtävillä palvelunestohyökkäyksillä	8.1	Lähetetään ajoneuvon tietojärjestelmään suuria määriä roskadataa, jolloin järjestelmä ei pysty tarjoamaan palveluja tavanomaisella tavalla.
			8.2	Hyökkääjä häiritsee ajoneuvojen välistä viestintää black hole -reitityshyökkäyksellä, jolloin hän pystyy estämään viestien siirtymisen ajoneuvojen välillä.
	9	Etuoikeudeton käyttäjä voi saada etuoikeutetun pääsyn ajoneuvojen järjestelmiin.	9.1	Etuoikeudeton käyttäjä voi saada etuoikeutetun käyttäjän aseman, esimerkiksi pääkäyttäjän oikeudet.
	10	Viestintävälineisiin upotetut virukset voivat saastuttaa ajoneuvon järjestelmiä.	10.1	Viestintävälineisiin upotettu virus saastuttaa ajoneuvon järjestelmät.
	11	Ajoneuvon vastaanottamissa (esim. X2V- tai vianmäärityssanomat) tai sen sisällä lähetetyissä viesteissä on haitallista sisältöä.	11.1	Haitalliset sisäiset viestit (esim. CAN).
			11.2	Haitalliset V2X-viestit esim. infrastruktuurista ajoneuvoon tai ajoneuvosta ajoneuvoon (esim. CAM, DENM).
			11.3	Haitalliset vianmäärityssanomat.
			11.4	Haitalliset valmistajaviestit (esim. viestit, joiden lähettäjä on yleensä alkuperäinen laitevalmistaja tai komponentin, järjestelmän tai toiminnon toimittaja).
4.3.3. Ajoneuvoihin kohdistuvat päivityksiin liittyvät uhkat	12	Päivitysmenettelyjen väärinkäyttö tai vaarantaminen	12.1	Langattomien ohjelmistopäivitysmenettelyjen vaarantaminen, kuten järjestelmäpäivitysohjelmiston tai kiinteän ohjelmiston väärentäminen.
			12.2	Paikallisten tai fyysisten ohjelmistopäivitysmenettelyjen vaarantaminen, kuten järjestelmäpäivitysohjelmiston tai kiinteän ohjelmiston väärentäminen.
			12.3	Ohjelmistoa peukaloidaan ennen päivitysprosessia (joten se on vioittunut), mutta itse päivitysprosessi on kunnossa.
			12.4	Heikennetään ohjelmistotoimittajan salausavaimia, jotta voidaan tehdä väärä päivitys.
	13	Mahdollisuus estää viralliset päivitykset	13.1	Kohdistetaan päivityspalvelinta tai -verkkoa vastaan palvelunestohyökkäys, jolla estetään kriittisten ohjelmistopäivitysten suorittaminen ja/tai lukittujen asiakaskohtaisten ominaisuuksien avaaminen.
4.3.4. Ajoneuvoihin kohdistuvat uhkat, jotka liittyvät kyberhyök-käyksiä helpottaviin tahattomiin ihmisen toimiin	15	Käyttöoikeuksin varustetut henkilöt voivat toteuttaa toimia, jotka saattavat vahingossa helpottaa kyberhyökkäyksen tekemistä.	15.1	Uhri (esim. omistaja, käyttäjä tai huoltomekaanikko) huijataan toteuttamaan toimi, jolla hän tahattomasti lataa haittaohjelman tai mahdollistaa hyökkäyksen.
			15.2	Määriteltyjä turvamenettelyjä ei noudateta.

Ylä- ja alatason kuvaus haavoittuvuudesta/uhkasta			Esimerkki haavoittuvuudesta tai hyökkäysmenetelmästä	
4.3.5. Ajoneuvoihin niiden ulkoisen liitettävyyden ja ulkoisten liitäntöjen kautta kohdistuvat uhkat	16	Kyberhyökkäyksen mahdollistaminen manipuloimalla ajoneuvon toimintojen liitettävyyttä, esim. telematiikkaa, etäkäytön mahdollistavia järjestelmiä ja lyhyen kantaman langatonta viestintää käyttäviä järjestelmiä	16.1	Manipuloidaan toimintoja, jotka liittyvät järjestelmien etäkäyttöön, kuten kaukosäädinavain, ajonestolaite tai latausparisto.
			16.2	Manipuloidaan ajoneuvon telematiikkaa (esim. lämpötilalle herkkien tavaroiden lämpötilan mittauksen manipulointi, tavaratilojen ovien kaukoohjattu avaaminen).
			16.3	Häiritään lyhyen kantaman langattomia järjestelmiä tai antureita.
	17	Ajoneuvojärjestelmiin kohdistettu hyökkäys, jossa hyödynnetään ajoneuvossa olevia kolmansien osapuolten järjestelmiä, kuten viihdesovelluksia	17.1	Kohdistetaan ajoneuvojärjestelmiin hyökkäys korruptoituneiden tai ohjelmistoturvallisuudeltaan heikkojen sovellusten kautta.
	18	Ajoneuvojärjestelmiin kohdistettu hyökkäys, jossa hyödynnetään ulkoisiin liitäntöihin (esim. USB- tai OBD-porttiin) kytkettyjä laitteita	18.1	Käytetään ulkoisia liitäntöjä, kuten USB- tai muita portteja hyökkäysväylänä esimerkiksi syöttämällä koodia niiden kautta.
			18.2	Ajoneuvojärjestelmään liitetään tallennusväline, joka sisältää viruksen.
			18.3	Käytetään vianmääritysyhteyttä (esim. OBD-porttiin liitettyä suojausavainta) helpottamaan hyökkäystä, esim. ajoneuvon parametrien manipulointiin (suoraan tai epäsuorasti).
4.3.6. Ajoneuvon dataan/ koodiin kohdistuvat uhkat	19	Ajoneuvon datan/koodin poimiminen	19.1	Tekijänoikeussuojattujen tai omisteisten ohjelmistojen poimiminen ajoneuvojärjestelmistä (tuotepiratismi)
			19.2	Luvaton pääsy omistajan yksityisyyden suojan piiriin kuuluviin tietoihin, kuten henkilöllisyys, maksutilitiedot, osoitekirja, paikkatiedot, ajoneuvon sähköinen tunniste jne.
			19.3	Salausavaimien kopiointi
	20	Ajoneuvon datan/koodin manipulointi	20.1	Laittomat/luvattomat muutokset ajoneuvon sähköiseen tunnisteeseen
			20.2	Henkilöllisyyspetos. Esimerkki: käyttäjä esittää toisen henkilöllisyyden yhteyksissään tiemaksujärjestelmiin tai valmistajan taustajärjestelmiin.
			20.3	Toimet seurantajärjestelmien kiertämiseksi (kuten viestien hakkerointi, luvaton muuntaminen tai estäminen, esim. ajotietotallentimen tiedot, ajojen lukumäärä)
			20.4	Tietojen manipulointi ajoneuvon ajotietojen väärentämiseksi (esim. ajokilometrit, ajonopeus, reitti)
			20.5	Luvattomat muutokset järjestelmän vianmääritystietoihin
	21	Tietojen tai koodin poistaminen	21.1	Järjestelmän tapahtumalokien luvaton poistaminen tai manipulointi
	22	Haittakoodin syöttäminen	22.2	Syötetään haittaohjelma tai aiheutetaan ohjelman haitallinen toiminta.

Ylä- ja alatason kuvaus haavoittuvuudesta/uhkasta			Esimerkki haavoittuvuudesta tai hyökkäysmenetelmästä	
	23	Uusien ohjelmien lataaminen tai olemassa olevien ohjelmien korvaaminen	23.1	Väärennetään ajoneuvon hallinta- tai tietojärjestelmän ohjelmistoja.
	24	Järjestelmien tai toimintojen häirintä	24.1	Aiheutetaan palvelunesto esimerkiksi sisäiseen verkkoon ruuhkauttamalla CAN-väylä tai aiheuttamalla viestitulvalla virhetoimintoja elektroniseen ohjausyksikköön.
	25	Ajoneuvon parametrien manipulointi	25.1	Hankitaan luvaton pääsy ja peukaloidaan ajoneuvon keskeisten toimintojen konfiguraatioparametreja, kuten jarrutietoja, turvatyynyn laukaisukynnystä jne.
			25.2	Hankitaan luvaton pääsy ja peukaloidaan latausparametreja, kuten latausjännitettä, lataustehoa, akun lämpötilaa jne.
4.3.7. Mahdolliset haavoittuvuudet, joita voidaan hyödyntää, ellei suojaus ole riittävä tai sitä ei paranneta	26	Salausteknologioiden turvallisuus voidaan vaarantaa tai niitä ei käytetä riittävästi.	26.1	Salausavaimien lyhyys ja pitkä voimassaoloaika antaa hyökkääjälle mahdollisuuden murtaa salaus.
			26.2	Arkaluontoisten järjestelmien suojaamiseen ei käytetä riittävästi salausalgoritmeja.
			26.3	Käytetään vanhentuneita tai pian vanhentuvia salausalgoritmeja.
	27	Osien tai tarvikkeiden turvallisuus voi vaarantua siten, että ajoneuvoon voidaan kohdistaa hyökkäys.	27.1	Laitteita tai ohjelmia muokataan hyökkäyksen mahdollistamiseksi, tai ne eivät täytä hyökkäyksen pysäyttämiseksi tarvittavia suunnittelukriteerejä.
	28	Ohjelmien tai laitteiden suunnittelu aiheuttaa haavoittuvuuksia.	28.1	Ohjelmistovirheet. Ohjelmistovirheet voivat aiheuttaa hyödynnettävissä olevia haavoittuvuuksia. Tämä on mahdollista erityisesti silloin, kun ohjelmistoa ei ole testattu tunnettujen virhekoodien ja virheiden varalta ja tuntemattomien virhekoodien ja virheiden esiintymisriskin pienentämiseksi.
			28.2	Kehittämisvaiheesta on voinut jäädä välineitä (esim. virheenkorjausportit, JTAG-portit, mikroprosessorit, kehittämisvaiheen oikeellisuustodistukset, kehittäjien salasanat), joiden avulla hyökkääjä voi saada pääsyn elektroniseen ohjausyksikköön tai hankkia laajempia käyttöoikeuksia.
	29	Verkon rakenne aiheuttaa haavoittuvuuksia.	29.1	Ylimääräiset auki jätetyt verkkoportit tarjoavat pääsyn verkkojärjestelmiin.
			29.2	Kierretään verkkojen erottelu hallinnan saamiseksi. Käytetään esimerkiksi suojaamattomia yhdyskäytäviä tai liitäntäpisteitä (kuten kuorma-autojen ja perävaunujen yhdyskäytäviä) suojausten kiertämiseksi ja muiden verkkosegmenttien ottamiseksi haltuun, jotta voidaan suorittaa vihamielisiä toimia, esim. lähettää sattumanvaraisia viestejä CAN-väylän kautta.
	31	Mahdolliset tahattomat tiedonsiirrot	31.1	Tietosuojaloukkaus. Henkilötietoja voi vuotaa, kun auto vaihtaa käyttäjää (esim. kun se myydään tai vuokra-ajoneuvon vuokraaja vaihtuu).

Ylä- ja alatason kuvaus haavoittuvuudesta/uhkasta			Esimerkki haavoittuvuudesta tai hyökkäysmenetelmästä	
	32	Järjestelmien fyysinen manipulointi voi mahdollistaa hyökkäyksen.	32.1	Manipuloidaan sähköisiä laitteita: esim. lisätään ajoneuvoon luvattomia elektronisia laitteita, jotka mahdollistavat väliintulohyökkäyksen. Vaihdetaan luvallinen elektroninen laite (esim. anturi) luvattomaan. Manipuloidaan anturin keräämiä tietoja (esim. häiritsemällä vaihdelaatikkoon yhdistettyä Hall-anturia magneetilla).

OSA B

Ajoneuvoihin kohdistuvien uhkien lieventämistoimenpiteet

1. Ajoneuvon viestintäkanavia koskevat lieventämistoimenpiteet

Taulukossa B1 luetellaan ajoneuvon viestintäkanaviin liittyvien uhkien lieventämistoimenpiteet.

Taulukko B1

Ajoneuvon viestintäkanaviin liittyvien uhkien lieventämistoimenpiteet

Viite taulukossa A1	Ajoneuvon viestintäkanaviin kohdistuvat uhkat	Viite	Lieventämistoimenpide
4.1	Viestejä väärennetään esiintymällä toisena henkilönä (esim. yhteistoiminnalliseen tietoisuuteen tai ajoliikkeiden koordinointiin käytettävät ajoneuvon ja toisen ajoneuvon tai muun tahon väliset V2X-viestit (CAM, MCM), GNSS-viestit jne.).	M10	Ajoneuvo tarkastaa saamiensa viestien aitouden ja eheyden.
4.2	Sybil-hyökkäys (muiden ajoneuvojen annetaan ymmärtää, että tiellä on useita ajoneuvoja)	M11	Salausavaimien säilyttämisessä käytetään turvavalvontatoimia (esim. laitteistoturvamoduulit).
5.1	Viestintäkanavien kautta voidaan syöttää ajoneuvossa olevaan dataan/koodiin koodia, esimerkiksi muunneltua binaarikoodia viestiliikenteeseen.	M10 M6	Ajoneuvo tarkastaa saamiensa viestien aitouden ja eheyden. Järjestelmissä on riskien minimoimiseksi noudatettava sisäänrakennetun turvallisuuden periaatetta.
5.2	Viestintäkanavien kautta voidaan manipuloida ajoneuvossa säilytettävää koodia/dataa.	M7	Järjestelmän datan/koodien suojaamiseksi käytetään pääsynvalvontatekniikoita ja -järjestelyjä.
5.3	Viestintäkanavien kautta voidaan korvata ajoneuvossa säilytettävää koodia/dataa.		
5.4 21.1	Viestintäkanavien kautta voidaan poistaa ajoneuvossa säilytettävää koodia/dataa.		
5.5	Viestintäkanavien kautta voidaan syöttää dataa/koodia ajoneuvojärjestelmiin (kirjoittaa dataa/koodia).		

Viite taulukossa A1	Ajoneuvon viestintäkanaviin kohdistuvat uhkat	Viite	Lieventämistoimenpide
6.1	Hyväksytään tietoja epäluotettavasta lähteestä.	M10	Ajoneuvo tarkastaa saamiensa viestien aitouden ja eheyden.
6.2	Väliintulohyökkäys / istunnon kaappaaminen	M10	Ajoneuvo tarkastaa saamiensa viestien aitouden ja eheyden.
6.3	Toistohyökkäys: hyökkääjä voi esimerkiksi viestintäväylään kohdistetun hyökkäyksen avulla heikentää elektronisen ohjausyksikön ohjelmistoa tai väylässä käytettävää laiteohjelmistoa.		
7.1	Tietojen sieppaaminen / häiritsevä säteily / viestinnän kuuntelu	M12	Ajoneuvoon tai ajoneuvosta siirretyt salassa pidettävät tiedot suojataan.
7.2	Hankitaan luvaton pääsy tiedostoihin tai tietoihin.	M8	Järjestelmän suunnittelun ja pääsynvalvonnan olisi estettävä valtuuttamattomien työntekijöiden pääsy henkilötietoihin tai järjestelmän kannalta kriittisiin tietoihin. Turvavalvontatoimenpiteistä annetaan esimerkkejä OWASP-hankkeessa.
8.1	Lähetetään ajoneuvon tietojärjestelmään suuria määriä roskadataa, jolloin järjestelmä ei pysty tarjoamaan palveluja tavanomaisella tavalla.	M13	Toteutetaan toimenpiteitä, joilla havaitaan palvelunestohyökkäys ja palautetaan toimintakunto sen jälkeen.
8.2	Hyökkääjä häiritsee ajoneuvojen välistä viestintää black hole -reitityshyökkäyksellä, jolla estetään viestien siirtäminen toisiin ajoneuvoihin.	M13	Toteutetaan toimenpiteitä, joilla havaitaan palvelunestohyökkäys ja palautetaan toimintakunto sen jälkeen.
9.1	Etuoikeudeton käyttäjä voi saada etuoikeutetun käyttäjän aseman, esimerkiksi pääkäyttäjän oikeudet.	M9	Toteutetaan toimenpiteitä, joilla estetään ja havaitaan luvaton pääsy.
10.1	Viestintävälineisiin upotettu virus saastuttaa ajoneuvon järjestelmät.	M14	Harkitaan toimenpiteitä järjestelmien suojaamiseksi upotetuilta viruksilta/ haittaohjelmilta.
11.1	Haitalliset sisäiset viestit (esim. CAN).	M15	Harkitaan toimenpiteitä haitallisten sisäisten viestien havaitsemiseksi.
11.2	Haitalliset V2X-viestit esim. infrastruktuurista ajoneuvoon tai ajoneuvosta ajoneuvoon (esim. CAM, DENM).	M10	Ajoneuvo tarkastaa saamiensa viestien aitouden ja eheyden.
11.3	Haitalliset vianmäärityssanomat.		
11.4	Haitalliset valmistajaviestit (esim. viestit, joiden lähettäjä on yleensä alkuperäinen laitevalmistaja tai komponentin, järjestelmän tai toiminnon toimittaja).		

2. Päivitysprosessiin liittyvät lieventämistoimenpiteet

Taulukossa B2 luetellaan päivitysprosesseihin kohdistuvien uhkien lieventämistoimenpiteet.

Taulukko B2

Päivitysprosesseihin kohdistuvien uhkien lieventämistoimenpiteet

Viite taulukossa A1	Päivitysprosessiin kohdistuvat uhkat	Viite	Lieventämistoimenpide
12.1	Langattomien ohjelmistopäivitysmenettelyjen vaarantaminen, kuten järjestelmäpäivitysohjelmiston tai kiinteän ohjelmiston väärentäminen.	M16	Käytetään suojattuja ohjelmistopäivitysmenettelyjä.
12.2	Paikallisten tai fyysisten ohjelmistopäivitysmenettelyjen vaarantaminen, kuten järjestelmäpäivitysohjelmiston tai kiinteän ohjelmiston väärentäminen.		
12.3	Ohjelmistoa peukaloidaan ennen päivitysprosessia (joten se on vioittunut), mutta itse päivitysprosessi on kunnossa.		
12.4	Heikennetään ohjelmistotoimittajan salausavaimia, jotta voidaan tehdä väärä päivitys.	M11	Salausavaimien säilyttämisessä käytetään turvavalvontatoimia.
13.1	Kohdistetaan päivityspalvelinta tai -verkkoa vastaan palvelunestohyökkäys, jolla estetään kriittisten ohjelmistopäivitysten suorittaminen ja/tai lukittujen asiakaskohtaisten ominaisuuksien avaaminen.	M3	Taustajärjestelmiin sovelletaan turvavalvontatoimenpiteitä. Kun taustapalvelimet ovat palvelujen tarjoamisen kannalta kriittisiä, järjestelmän käyttökatkon varalta on olemassa palautusmenettelyjä. Turvavalvontatoimenpiteistä annetaan esimerkkejä OWASP-hankkeessa.

3. Lieventämistoimenpiteet, jotka liittyvät kyberhyökkäyksiä helpottaviin tahattomiin ihmisen toimiin

Taulukossa B3 luetellaan lieventämistoimenpiteet, jotka liittyvät kyberhyökkäyksiä helpottaviin tahattomiin ihmisen toimiin.

Taulukko B3

Lieventämistoimenpiteet, jotka liittyvät kyberhyökkäyksiä helpottaviin tahattomiin ihmisen toimiin

Viite taulukossa A1	Tahattomiin ihmisen toimiin liittyvät uhkat	Viite	Lieventämistoimenpide
15.1	Uhri (esim. omistaja, käyttäjä tai huoltomekaanikko) huijataan toteuttamaan toimi, jolla hän tahattomasti lataa haittaohjelman tai mahdollistaa hyökkäyksen.	M18	Toteutetaan toimenpiteitä käyttäjäroolien ja käyttöoikeuksien määrittelemiseksi ja valvomiseksi pienimpien käyttöoikeuksien periaatteen mukaisesti.

Viite taulukossa A1	Tahattomiin ihmisen toimiin liittyvät uhkat	Viite	Lieventämistoimenpide
15.2	Määriteltyjä turvamenettelyjä ei noudateta.	M19	Organisaatiot varmistavat, että turvamenettelyt määritellään ja niitä noudatetaan, mukaan luettuna turvallisuustoimintojen hallinnointiin liittyvien toimien ja käyttöoikeuksien käytön kirjaaminen.

4. Ulkoiseen liitettävyyteen ja ulkoisiin liitäntöihin liittyvät lieventämistoimenpiteet

Taulukossa B4 luetellaan ulkoiseen liitettävyyteen ja ulkoisiin liitäntöihin liittyvien uhkien lieventämistoimenpiteet.

Taulukko B4

Ulkoiseen liitettävyyteen ja ulkoisiin liitäntöihin liittyvien uhkien lieventämistoimenpiteet

Viite taulukossa A1	Ulkoiseen liitettävyyteen ja ulkoisiin liitäntöihin liittyvät uhkat	Viite	Lieventämistoimenpide
16.1	Manipuloidaan toimintoja, jotka liittyvät järjestelmien etäkäyttöön, kuten kaukosäädinavain, ajonestolaite tai latausparisto.	M20	Etäkäytöllä varustettuihin järjestelmiin sovelletaan turvavalvontatoimenpiteitä.
16.2	Manipuloidaan ajoneuvon telematiikkaa (esim. lämpötilalle herkkien tavaroiden lämpötilan mittauksen manipulointi, tavaratilojen ovien kauko-ohjattu avaaminen).		
16.3	Häiritään lyhyen kantaman langattomia järjestelmiä tai antureita.		
17.1	Kohdistetaan ajoneuvojärjestelmiin hyökkäys korruptoituneiden tai ohjelmistoturvallisuudeltaan heikkojen sovellusten kautta.	M21	Ohjelmistoista on tehtävä turvallisuusarvio, ne on varmennettava, ja niiden eheys on suojattava. Turvavalvontatoimenpiteillä on minimoitava sellaisten kolmansien osapuolten ohjelmistojen aiheuttama riski, joiden isännöinti ajoneuvossa on suunniteltua tai ennakoitavissa.
18.1	Käytetään ulkoisia liitäntöjä, kuten USB- tai muita portteja hyökkäysväylänä esimerkiksi syöttämällä koodia niiden kautta.	M22	Ulkoisiin liitäntöihin sovelletaan turvavalvontatoimenpiteitä.
18.2	Ajoneuvoon liitetään tallennusväline, joka sisältää viruksen.		
18.3	Käytetään vianmääritysyhteyttä (esim. OBD-porttiin liitettyä suojausavainta) helpottamaan hyökkäystä, esim. ajoneuvon parametrien manipulointiin (suoraan tai epäsuorasti).	M22	Ulkoisiin liitäntöihin sovelletaan turvavalvontatoimenpiteitä.

5. Lieventämistoimenpiteet, jotka koskevat hyökkäyksen mahdollisia kohteita tai syitä

Taulukossa B5 luetellaan lieventämistoimenpiteet, jotka koskevat hyökkäyksen mahdollisiin kohteisiin tai syihin liittyviä uhkia.

Taulukko B5

Lieventämistoimenpiteet, jotka koskevat hyökkäyksen mahdollisiin kohteisiin tai syihin liittyviä uhkia

Viite taulukossa A1	Uhkat, jotka liittyvät hyökkäyksen mahdollisiin kohteisiin tai syihin	Viite	Lieventämistoimenpide
19.1	Tekijänoikeussuojattujen tai omisteisten ohjelmistojen noutaminen ajoneuvojärjestelmistä (tuotepiratismi / anastettu ohjelmisto)	M7	Järjestelmän datan/koodien suojaamiseksi käytetään pääsynvalvontatekniikoita ja -järjestelyjä. Turvavalvontatoimenpiteistä annetaan esimerkkejä OWASP-hankkeessa.
19.2	Luvaton pääsy omistajan yksityisyyden suojan piiriin kuuluviin tietoihin, kuten henkilöllisyys, maksutilitiedot, osoitekirja, paikkatiedot, ajoneuvon sähköinen tunniste jne.	M8	Järjestelmän suunnittelun ja pääsynvalvonnan olisi estettävä valtuuttamattomien työntekijöiden pääsy henkilötietoihin tai järjestelmän kannalta kriittisiin tietoihin. Turvavalvontatoimenpiteistä annetaan esimerkkejä OWASP-hankkeessa.
19.3	Salausavaimien kopiointi	M11	Salausavaimien säilyttämisessä käytetään turvavalvontatoimia esim. turvamoduuleja.
20.1	Laittomat/luvattomat muutokset ajoneuvon sähköiseen tunnisteeseen	M7	Järjestelmän datan/koodien suojaamiseksi käytetään pääsynvalvontatekniikoita ja -järjestelyjä. Turvavalvontatoimenpiteistä annetaan esimerkkejä OWASP-hankkeessa.
20.2	Henkilöllisyyspetos. Esimerkki: käyttäjä esittää toisen henkilöllisyyden yhteyksissään tiemaksujärjestelmiin tai valmistajan taustajärjestelmiin.		
20.3	Toimet seurantajärjestelmien kiertämiseksi (kuten viestien hakkerointi, luvaton muuntaminen tai estäminen, esim. ajotietotallentimen tiedot, ajojen lukumäärä)	M7	Järjestelmän datan/koodien suojaamiseksi käytetään pääsynvalvontatekniikoita ja -järjestelyjä. Turvavalvontatoimenpiteistä annetaan esimerkkejä OWASP-hankkeessa. Antureihin tai siirrettyihin tietoihin kohdistuvia datamanipulointiuhkia voidaan lieventää eri tietolähteistä tulevan datan korreloinnilla.
20.4	Tietojen manipulointi ajoneuvon ajotietojen väärentämiseksi (esim. ajokilometrit, ajonopeus, reitti)		
20.5	Luvattomat muutokset järjestelmän vianmääritystietoihin		
21.1	Järjestelmän tapahtumalokien luvaton poistaminen tai manipulointi	M7	Järjestelmän datan/koodien suojaamiseksi käytetään pääsynvalvontatekniikoita ja -järjestelyjä. Turvavalvontatoimenpiteistä annetaan esimerkkejä OWASP-hankkeessa.
22.2	Syötetään haittaohjelma tai aiheutetaan ohjelman haitallinen toiminta.	M7	Järjestelmän datan/koodien suojaamiseksi käytetään pääsynvalvontatekniikoita ja -järjestelyjä. Turvavalvontatoimenpiteistä annetaan esimerkkejä OWASP-hankkeessa.
23.1	Väärennetään ajoneuvon hallinta- tai tietojärjestelmän ohjelmistoja.		

Viite taulukossa A1	Uhkat, jotka liittyvät hyökkäyksen mahdollisiin kohteisiin tai syihin	Viite	Lieventämistoimenpide
24.1	Aiheutetaan palvelunesto esimerkiksi sisäiseen verkkoon ruuhkauttamalla CAN-väylä tai aiheuttamalla viestitulvalla virhetoimintoja elektroniseen ohjausyksikköön.	M13	Toteutetaan toimenpiteitä, joilla havaitaan palvelunestohyökkäys ja palautetaan toimintakunto sen jälkeen.
25.1	Hankitaan luvaton pääsy ja peukaloidaan ajoneuvon keskeisten toimintojen konfiguraatioparametreja, kuten jarrutietoja, turvatyynyn laukaisukynnystä jne.	M7	Järjestelmän datan/koodien suojaamiseksi käytetään pääsynvalvontatekniikoita ja -järjestelyjä. Turvavalvontatoimenpiteistä annetaan esimerkkejä OWASP-hankkeessa.
25.2	Hankitaan luvaton pääsy ja peukaloidaan latausparametreja, kuten latausjännitettä, lataustehoa, akun lämpötilaa jne.		

6. Lieventämistoimenpiteet, jotka koskevat mahdollisia haavoittuvuuksia, joita voidaan hyödyntää, ellei suojaus ole riittävä tai sitä ei paranneta

Taulukossa B6 esitetään sellaisia uhkia koskevat lieventämistoimenpiteet, jotka koskevat mahdollisia haavoittuvuuksia, joita voidaan hyödyntää, ellei suojaus ole riittävä tai sitä ei paranneta.

Taulukko B6

Sellaisia uhkia koskevat lieventämistoimenpiteet, jotka koskevat mahdollisia haavoittuvuuksia, joita voidaan hyödyntää, ellei suojaus ole riittävä tai sitä ei paranneta

Viite taulukossa A1	Uhkat, jotka koskevat mahdollisia haavoittuvuuksia, joita voidaan hyödyntää, ellei suojaus ole riittävä tai sitä ei paranneta	Viite	Lieventämistoimenpide
26.1	Salausavaimien lyhyys ja pitkä voimassaoloaika antaa hyökkääjälle mahdollisuuden murtaa salaus.	M23	Noudatetaan kyberturvallisuuden parhaita käytäntöjä ohjelmistojen ja laitteistojen kehittämisessä.
26.2	Arkaluontoisten järjestelmien suojaamiseen ei käytetä riittävästi salausalgoritmeja.		
26.3	Käytetään vanhentuneita salausalgoritmeja.		
27.1	Laitteita tai ohjelmia muokataan hyökkäyksen mahdollistamiseksi, tai ne eivät täytä hyökkäyksen pysäyttämiseksi tarvittavia suunnittelukriteerejä.	M23	Noudatetaan kyberturvallisuuden parhaita käytäntöjä ohjelmistojen ja laitteistojen kehittämisessä.
28.1	Ohjelmistovirheet voivat aiheuttaa hyödynnettävissä olevia haavoittuvuuksia. Tämä on mahdollista erityisesti silloin, kun ohjelmistoa ei ole testattu tunnettujen virhekoodien ja virheiden varalta ja tuntemattomien virhekoodien ja virheiden esiintymisriskin pienentämiseksi.	M23	Noudatetaan kyberturvallisuuden parhaita käytäntöjä ohjelmistojen ja laitteistojen kehittämisessä. Tehdään riittävän laajuisia kyberturvallisuustestejä.

Viite taulukossa A1	Uhkat, jotka koskevat mahdollisia haavoittuvuuksia, joita voidaan hyödyntää, ellei suojaus ole riittävä tai sitä ei paranneta	Viite	Lieventämistoimenpide
28.2	Kehittämisvaiheesta on voinut jäädä välineitä (esim. virheenkorjausportit, JTAG-portit, mikroprosessorit, kehittämisvaiheen oikeellisuustodistukset, kehittäjien salasanat), joiden avulla hyökkääjä voi saada pääsyn elektroniseen ohjausyksikköön tai hankkia laajempia käyttöoikeuksia.		
29.1	Ylimääräiset auki jätetyt verkkoportit tarjoavat pääsyn verkkojärjestelmiin.		
29.2	Kierretään verkkojen erottelu hallinnan saamiseksi. Käytetään esimerkiksi suojaamattomia yhdyskäytäviä tai liitäntäpisteitä (kuten kuorma-autojen ja perävaunujen yhdyskäytäviä) suojausten kiertämiseksi ja muiden verkkosegmenttien ottamiseksi haltuun, jotta voidaan suorittaa vihamielisiä toimia, esim. lähettää sattumanvaraisia viestejä CAN-väylän kautta.	M23	Noudatetaan kyberturvallisuuden parhaita käytäntöjä ohjelmistojen ja laitteistojen kehittämisessä. Noudatetaan järjestelmien suunnittelun ja integroinnin parhaita käytäntöjä.

7. Ajoneuvon tietojen katoamista tai niihin liittyvää tietosuojaloukkausta koskevat lieventämistoimenpiteet

Taulukossa B7 luetellaan ajoneuvon tietojen katoamista tai niihin liittyvää tietosuojaloukkausta koskevien uhkien lieventämistoimenpiteet.

Taulukko B7

Ajoneuvon tietojen katoamista tai niihin liittyvää tietosuojaloukkausta koskevien uhkien lieventämistoimenpiteet

Viite taulukossa A1	Ajoneuvon tietojen katoamista tai niihin liittyvää tietosuojaloukkausta koskevat uhkat	Viite	Lieventämistoimenpide
31.1	Tietosuojaloukkaus. Henkilötietoja voi vuotaa, kun auto vaihtaa käyttäjää (esim. kun se myydään tai vuokra-ajoneuvon vuokraaja vaihtuu)	M24	Henkilötietojen säilyttämisessä noudatetaan tietojen eheyden ja luottamuksellisuuden suojaamista koskevia parhaita käytäntöjä.

8. Lieventämistoimenpiteet, jotka koskevat hyökkäyksen mahdollistavaa järjestelmien fyysistä manipulointia

Taulukossa B8 luetellaan lieventämistoimenpiteet, jotka koskevat hyökkäyksen mahdollistavaan järjestelmien fyysiseen manipulointiin liittyviä uhkia.

Taulukko B8

Lieventämistoimenpiteet, jotka koskevat hyökkäyksen mahdollistavaan järjestelmien fyysiseen manipulointiin liittyviä uhkia

Viite taulukossa A1	Uhkat, jotka koskevat hyökkäyksen mahdollistavaa järjestelmien fyysistä manipulointia	Viite	Lieventämistoimenpide
32.1	Manipuloidaan alkuperäisen laitevalmistajan toimittamia laitteita: esim. lisätään ajoneuvoon luvattomia elektronisia laitteita, jotka mahdollistavat väliintulohyökkäyksen.	M9	Toteutetaan toimenpiteitä, joilla estetään ja havaitaan luvaton pääsy.

OSA C

Ajoneuvon ulkopuolisten uhkien lieventämistoimenpiteet

1. Taustapalvelimiin liittyvät lieventämistoimenpiteet

Taulukossa C1 luetellaan taustapalvelimiin kohdistuvien uhkien lieventämistoimenpiteet.

Taulukko C1

Taustapalvelimiin kohdistuvien uhkien lieventämistoimenpiteet

Viite taulukossa A1	Taustapalvelimiin liittyvät uhkat	Viite	Lieventämistoimenpide
1.1 & 3.1	Henkilöstö käyttää oikeuksiaan väärin (sisäpiirihyökkäys).	M1	Taustapalvelimiin sovelletaan turvavalvontatoimenpiteitä sisäpiirihyökkäyksen riskin minimoimiseksi.
1.2 & 3.3	Palvelimeen otetaan luvaton internetyhteys (esimerkiksi hyödyntämällä takaportteja, paikkaamattomia järjestelmäohjelmistojen haavoittuvuuksia, SQL-hyökkäyksiä tai muita keinoja).	M2	Taustapalvelimiin sovelletaan turvavalvontatoimenpiteitä luvattomien yhteyksien minimoimiseksi. Turvavalvontatoimenpiteistä annetaan esimerkkejä OWASP-hankkeessa.
1.3 & 3.4	Palvelinta käytetään luvatta fyysisesti (esimerkiksi USB-muistitikulla tai muulla palvelimeen yhdistetyllä välineellä).	M8	Järjestelmän suunnittelun ja pääsynvalvonnan olisi estettävä valtuuttamattomien työntekijöiden pääsy henkilötietoihin tai järjestelmän kannalta kriittisiin tietoihin.
2.1	Hyökkäys taustapalvelimeen pysäyttää sen toiminnan ja esimerkiksi estää sitä toimimasta vuorovaikutuksessa ajoneuvojen kanssa ja tarjoamaan niille niiden tarvitsemia palveluja.	M3	Taustajärjestelmiin sovelletaan turvavalvontatoimenpiteitä. Kun taustapalvelimet ovat palvelujen tarjoamisen kannalta kriittisiä, järjestelmän käyttökatkon varalta on olemassa palautusmenettelyjä. Turvavalvontatoimenpiteistä annetaan esimerkkejä OWASP-hankkeessa.
3.2	Pilvipalveluissa olevat tiedot katoavat. Hyökkäysten tai onnettomuuksien vuoksi voidaan menettää arkaluonteisia tietoja, joita säilytetään kolmannen osapuolen tarjoamissa pilvipalveluissa.	M4	Sovelletaan turvavalvontatoimenpiteitä pilvipalveluihin liittyvien riskien minimoimiseksi. Turvavalvontatoimenpiteistä annetaan esimerkkejä OWASP-hankkeessa ja NCSC:n pilvipalveluohjeissa.
3.5	Tietojen tahaton jakaminen vaarantaa tietosuojan (esim. hallinnolliset virheet tai tietojen säilyttäminen korjaamojen palvelimilla).	M5	Taustajärjestelmiin sovelletaan turvavalvontatoimenpiteitä tietosuojaloukkausten estämiseksi. Turvavalvontatoimenpiteistä annetaan esimerkkejä OWASP-hankkeessa.

2. Tahattomiin ihmisen toimiin liittyvät lieventämistoimenpiteet

Taulukossa C2 luetellaan tahattomiin ihmisen toimiin liittyvien uhkien lieventämistoimenpiteet.

Taulukko C2

Tahattomiin ihmisen toimiin liittyvien uhkien lieventämistoimenpiteet

Viite taulukossa A1	Tahattomiin ihmisen toimiin liittyvät uhkat	Viite	Lieventämistoimenpide
15.1	Uhri (esim. omistaja, käyttäjä tai huoltomekaanikko) huijataan toteuttamaan toimi, jolla hän tahattomasti lataa haittaohjelman tai mahdollistaa hyökkäyksen.	M18	Toteutetaan toimenpiteitä käyttäjäroolien ja käyttöoikeuksien määrittelemiseksi ja valvomiseksi pienimpien käyttöoikeuksien periaatteen mukaisesti.
15.2	Määriteltyjä turvamenettelyjä ei noudateta.	M19	Organisaatiot varmistavat, että turvamenettelyt määritellään ja niitä noudatetaan, mukaan luettuna turvallisuustoimintojen hallinnointiin liittyvien toimien ja käyttöoikeuksien käytön kirjaaminen.

3. Tietojen fyysiseen menettämiseen liittyvät lieventämistoimenpiteet

Taulukossa C3 luetellaan tietojen fyysiseen menettämiseen liittyvien uhkien lieventämistoimenpiteet.

Taulukko C3

Tietojen fyysiseen menettämiseen liittyvien uhkien lieventämistoimenpiteet

Viite taulukossa A1	Tietojen fyysiseen menettämiseen liittyvät uhkat	Viite	Lieventämistoimenpide
30.1	Kolmannen osapuolen aiheuttama vahinko. Fyysiset vauriot liikenneonnettomuuden tai varkauden yhteydessä voivat johtaa arkaluontoisten tietojen menettämiseen tai vaarantumiseen.	M24	Henkilötietojen säilyttämisessä noudatetaan tietojen eheyden ja luottamuksellisuuden suojaamista koskevia parhaita käytäntöjä. Turvavalvontatoimenpiteistä annetaan esimerkkejä asiakirjassa ISO/SC27/WG5.
30.2	Tietojen menettäminen digitaalisten oikeuksien hallintaan (DRM) liittyvien ristiriitojen vuoksi. Käyttäjätietoja voidaan poistaa DRM-ongelmien vuoksi.		
30.3	Arkaluontoisia tietoja voidaan menettää (tai niiden eheys voi kärsiä) komponenttien kulumisen vuoksi, millä voi olla kerrannaisvaikutuksia (esim. avainten muuttamisen tapauksessa).		