Tampereen yliopisto

Lassi Vuotari

# DO-178C STANDARDI MIEHITTÄMÄTTÖMIEN ILMA-ALUKSIEN NÄKÖKULMASTA

Kandidaattitutkielma
Informaatioteknologian ja viestinnän tiedekunta

Huhtikuu 2021

# TIIVISTELMÄ

Lassi Vuotari: DO-178C standardi miehittämättömien ilma-aluksien näkökulmasta
Kandidaattitutkielma
Tampereen yliopisto
Tieto- ja sähkötekniikan kandidaatin tutkinto-ohjelma
Tarkastaja: Matti Monnonen
Huhtikuu 2021

---

Kandidaatintyö käsittelee miehittämättömien ilma-alusten ohjelmistoturvallisuutta. Aihe on rajattu kaupallisessa siviili-ilmailukäytössä olevaan lentokalustoon. Ilmailujärjestelmät ovat tunnistettu omaksi erityiseksi kriittiseksi järjestelmäksi. Miehitetylle ilmailulle on luotu oma ohjelmistoturvallisuutta koskeva standardi, DO-178. Työn tavoite on tarkastella jo olemassa olevan miehitetyn ilmailun ohjelmistoturvallisuuden ohjenuorien soveltumista miehittämättömien ilma-alusten käyttöön. Tarkoituksena on arvioida standardiin siirtymisen soveltumista erityisluontoisuuden huomioiden, mahdollisuutta suoraan soveltamiseen lainsäädännön sekä viranomaistoiminnan näkökulmasta ja saavutettavissa olevia hyötyjä sekä kustannuksia alalla toimiville tahoille.

Työ jakautuu kolmeen osaan. Työn ensimmäisessä osassa tarkastellaan ilmailukriittisen ohjelmiston piirteitä. Ohjelmistojen tarpeista kerrotaan lainsäädännössä, valvovien viranomaisten dokumenteissa, kolmannen sektorin luomissa ohjeissa, sekä alan kirjallisuudessa. Toisessa osiossa työssä tutustutaan miehittämättömien ilma-alusten määritelmiin, toiminnan erityslaatuisuuden lokerointiin sekä eri alueiden viranomaisten näkemyksien eroihin. Määritelmistä tietoa saa valvovien viranomaisten ohjeista sekä paikallisesta lainsäädännöstä. Työn kolmannessa osiossa käsitellään miehittämättömien ilma-alusten ohjelmistoturvallisuustilannetta nyt sekä sitä, miten jo olemassa olevan standardin omaksuminen näkyisi alalla toimiville toimijoille. Tietoa nykytilanteesta saa lainsäädännöstä sekä viranomaisten ohjeistuksesta. Turvallisuuspoikkeamista sekä muutostarpeista saa tietoa uutisoiduista poikkeamista sekä viranomaisten pitämistä tiedotus- ja informointitilaisuuksista. Standardin omaksumisesta tietoa on tarjolla alan kirjallisuudesta, jossa reflektoidaan kokemuksia miehitetyn ilmailun osalta.

Tutkielman perusteella viranomaisilta on tullut ilmailuturvallisuuteen liittyviä vaatimuksia, joihin miehittämättömien ilma-alusten on mahdollista vastata miehitetyn ilmailun standardeilla. Standardiekosysteemiin siirtymisellä on saavutettavissa turvallisuusetuja sekä kilpailuetua monilla markkinoilla. Siirtymään liittyviä kustannuksia pystyy arvioimaan jo tapahtuneiden siirtymien perusteella.

Avainsanat: lennokki, UAV, drone, sulautetut järjestelmät, ohjelmistoturvallisuus, turvakriittinen

# ALKUSANAT

Haluan kiittää yliopisto-opettaja Matti Monnosta työn ohjauksesta ja tarkastuksesta.

Haluan kiittää kaikkia tahoja, jotka mahdollistavat vapaan pääsyn tieteellisiin teksteihin ja tietoon.

Tampereella, 22.04.2021

Lassi Vuotari

# SISÄLLYSLUETTELO

# LYHENTEET JA MERKINNÄT

| | |
|---|---|
| AC 20-115C | ilmailun ohjelmistokehityksen varmennuksen ohje |
| ARP | aerospace recommended practice |
| BVLOS | beyond visual line-of-sight |
| DAL | design assurance level |
| DO-178 | ilmailun ohjelmistosuunnittelun standardi |
| DO-330 | ilmailun ohjelmistotuotannon työkalujen laadunarviontiohje |
| EASA | Euroopan lentoturvallisuusvirasto |
| E-VLOS | extended visual line-of-sight |
| FAA | Yhdysvaltain ilmailuhallinto |
| IEC | international electrotechnical commission |
| ISO | international organization for standardization |
| OPS M1-32 | Traficomin määräys: *kauko-ohjatun ilma-aluksen ja lennokin käyttäminen ilmailuun* |
| RPA | remotely piloted aircraft |
| RPAS | remotely piloted aircraft system |
| RPS | remote pilot station |
| RTCA | radio technical commission for aeronautics |
| SAE International | society of automotive engineers, standardointijärjestö |
| UAS | unmanned aerial system |
| UAV | unmanned aerial vehicle |
| VLOS | visual line-of-sight |

# 1. JOHDANTO

Miehittämättömien kauko-ohjattavien ilma-alusten määrä on kasvanut huimasti ja todella nopeasti. Viidessä vuodessa markkinan rahallinen arvo oli kasvanut yli kymmenkertaiseksi. Näiden markkinoiden on myös projektoitu kasvavan alati kasvavaa tahtia. Nykyisin suurin kysyntä tulee harrastuksenomaisesta kuvaustoiminnasta. Tämä segmentti tulee analyysien mukaan kasvamaan varsin lineaarisesti. Suurinta kasvua haetaan kaupallisesta toiminnasta. Kasvavia kaupallisia käyttökohteita ovat yleinen kuvaustoiminta, kartoitus, kaavoitus, maatalous, tarkistus ja huoltotoiminta. [1]

Kuvaustoiminnan osalta suurin tunnistettu kasvava yksittäinen asiakassegmentti on prosumer-asiakas [1]. Prosumer on samanaikaisesti kuluttaja ja tuottaja. Käytännössä tässä kontekstissa nämä toimijat ovat hankkineet ilma-aluksen ensisijaisesti omaksi ilokseen, mutta toimivat myös palveluntarjoajina. Esimerkiksi prosumer saattaa kuvata YouTube-videoita tai kuvata naapuruston taloja myynti-ilmoituksiin.

Tämä luonnemuutos ilma-aluksien käytössä saattaa vaikuttaa varsin pieneltä, mutta Traficomin ilmailumääräys OPS M1-32 *kauko-ohjatun ilma-aluksen ja lennokin lennättäminen* sekä EU:n yhteisten dronesääntöjen mukainen määräys rinnastavat miehittämättömillä ilma-aluksilla kaupallisesti toimimisen lentotyöksi. [2] Lentotyötä koskee varsin mittava määrä määräyksiä ja toiminta vaatii lentotoimintaluvan. Tämä muutos myös altistaa lentokaluston, lentoa harjoittavan organisaation sekä luvan haltijan toiminnan yleisesti Traficomin vaatimuksille [3, 70 §].

Miehittämättömistä ilma-aluksista on yleistymisenkin mukaisesti tehty alati enemmän opinnäytetöitä sekä tutkimuksia. Tutkimukset sekä opinnäytetyöt ovat vahvasti keskittyneet tekniikan analysointiin, teknisten ratkaisujen tuottamiseen sekä eri tehtäviin soveltuvuuden arviointiin. Todella suuria muutosvoimia jyllää kaupallisella sektorilla. Kuluttajille ja prosumer-asiakkaille suunnattua kalustoa on tullut runsaasti ja kehitys on ollut huomattavaa [1].

Lentokaluston käytön luonne muuttuu, eikä suomen kielellä ole tehty tutkimusta kaluston ohjelmistojen sertifioinnista. Puolustussektorilla on tehty huomattavaa teknologista kehitystä. Tämän sektorin toimijat eivät valitettavasti jaa tutkimustietoaan kovin kernaasti, ja tutkimuksen tasoa on vaikea arvioida ulkoapäin. Puolustus- ja viranomaistoiminta onkin monesti rajattu normaalin ilmailulainsäädännön ulkopuolelle [3]. DO-178C koskee vain kaupallista ilmailukalustoa [4], vaikka sen periaatteita sovelletaan myös puolustussektorilla. Näistä syistä johtuen työ tarkastelee vain kaupalliseen siviili-ilmailuun käytettyä lentokalustoa.

Tässä turkielmassa tutustutaan miehittämättömien ilma-alusten ohjelmistoturvallisuuteen. Työn tarkoituksena on tutkia soveltuuko standardi DO-178C:n miehittämättömille ilma-aluksille.

Työssä tutustutaan ensiksi toisessa luvussa ilma-alusten ohjelmistojen turvakriittisyyden varmistamiseen nyt. Kolmas luku käsittelee miehittämättömiä ilma-aluksia sekä niihin liittyviä käsitteitä ja käytäntöjä tällä hetkellä merkittävimmillä markkina-alueilla. Luvussa tarkastellaan myös minkälaisia muutosprosesseja viranomaiset ovat aloittaneet liittyen miehittämättömiin ilma-aluksiin. Neljännessä

luvussa tarkastellaan nykyistä vaatimustasomenettelyä, mahdollisesti saavutettavissa olevaa hyötyä sekä mahdollisia haittapuolia. Lopuksi viides luku tekee yhteenvedon tutkielmasta.

# 2. TURVAKRIITTISET JÄRJESTELMÄT ILMAILUSSA

## 2.1 Turvakriittiset järjestelmät ja ohjelmointi

Turvakriittinen järjestelmä on järjestelmä, joka voisi virheen vuoksi aiheuttaa kuoleman, vakavan vamman, huomattavan määrän taloudellista vahinkoa tai vahingon ympäristölle. Nämä järjestelmät koostuvat laitteistosta, ohjelmistoista, ympäristöstä sekä käyttäjistä. [6] On tärkeää erottaa henkilöturvallisuus (eng. safety) kaikesta turvallisuuteen liittyvästä tekniikasta (eng. security). Etenkin henkilöturvallisuus halutaan taata. Turvallisuussuunnitteluprosessit ovat erilaisia riippuen kriittisyyden arvioidusta määrästä ja laadusta. [7]

Ohjelmistotuotantoa turvakriittisiin järjestelmiin säätelevät monet standardit. Tieliikenteessä seurataan ISO 26262:ta. [8] Autonominen tieliikenne onkin tuottanut painetta tarkastella tätä ISO-standardia varsin uudesta näkökulmasta, ja standardia on päivitetty varsin tiheään, viimeksi vuonna 2018 [9]. Lääketieteellisissä järjestelmissä seurataan IEC 62304:ää ja ydinvoimaan liittyen IEC 61513:a. Montaa alaa ei koeta kriittisyyden laadultaan sellaisiksi, että omaa standardia koettaisiin tarvittavan tai läsnä olevien haasteiden laatu ei ole harvinaisen erityisluontoista. Yleisstandardi ohjelmistotuotannolle turvakriittisille järjestelmille on IEC 61508. [8]

On kolme näkökulmaa, jotka tulee ottaa huomioon turvakriittisiä ohjelmistoja tuotettaessa. Järjestelmää suunniteltaessa ja prosessin johtamisessa tarvitsee huomioida käytön erityisluonne ja vaarallisuus. Toiseksi työkalut ja ympäristö täytyy valita järjestelmä huomioiden. Tämän lisäksi täytyy täyttää lailliset ja säädöksistä johtuvat vaatimukset. [5] On myös mahdollista pukea vaatimukset todistuksiksi, jotta voidaan osoittaa, että ohjelmisto vastaa vaatimuksiin. Tämä on ohjelmistojen elinkaarikustannusten kannalta varsin kustannustehokasta, jos testiympäristöt laaditaan kattaviksi jo tuotantoa varten. [10]

## 2.2 DO-178C

DO-178C on RTCA Inc.:n julkaisema dokumentti, joka on pääasiallinen kaupallisten lentoteknisten ohjelmistojen sertifiointiin käytetty ohjaava dokumentti. Dokumentin perusteella sertifioinnit antavat muun muassa FAA, EASA ja Kanadan liikenneviranomainen. [4] DO-178C on julkaistu ja hyväksytty RTCA:n toimesta joulukuussa 2011. Julkaisu korvasi edeltäneen ohjaavan dokumentin, DO-178B:n. FAA tunnisti DO-178C:n sopivaksi lentoteknisten ohjelmistojen arviointiin dokumentissaan AC 20-115C vuonna 2013. [11]

ARP4754A on SAE Internationalin tuottama lentokonejärjestelmien sertifiontiohje [12]. ARP4754A:ta on tarkoitus käyttää yhteisesti muiden ilmailuun liittyvien dokumenttien kanssa. Ohjeen tarkoitus on toimia turvallisuuden suunnittelu- ja testausprosessien kattavuuden takaamisessa. [11] DO-178 on yhtenäistänyt turvallisuusluokkansa ja terminologiansa ARP4754A:n kanssa [10]. DO-178 on osa tässä systemaattisessa

turvallisuusympäristössä. Luodun ympäristön tarkoitus olla järjestelmällisiä virheitä vähentävä [11] ja suuntaviivoitettu niin, että turvallisuustavoitteisiin on ohjelmistotuotannollisesti mahdollista päästä [12].

DO-178:aa luo seitsemän pienryhmää. Jokainen näistä työstää omaa osa-aluettaan. Nämä osa-alueet ovat toimitusketjun dokumentaation integraatio, ongelmanmäärittely ja ongelmien perustelut, työkalujen arviointi, mallipohjainen kehitys ja varmistus, olio-ohjelmointi, formaalit käytännöt sekä turvallisuuteen liittyvät pohdinnat. [10]

## 2.3 DO-178C:n ero DO-178B:hen

DO-178B on DO-178C:tä edeltänyt dokumentti, jolla oli ilmailuteollisuudessa vastaava asema [4]. Tämän dokumentin viimeisin iteraatio julkaistiin 1992 [11]. Näiden dokumenttien pitkäikäisyys on suurelta osin vahvan dokumentin auditointiprosessin sekä muutoksien kalleuden summa [13]. Muutoksiin vaikutti ilmailuteollisuuden muutos [13], havaitut epäkohdat [11] sekä ARP4754:n luomat järjestelmäsuunnitteluun liittyvien kriteerien määrittely [12].

DO-178C:hen on lisätty DO-178B:hen verrattuna enemmän tavoitteita D-tasoa kovemmille turvallisuusluokille [14]. Uudessa dokumentissa on yksiselitteisempi kieliasu ja terminologiaa on siivottu [11]. DO-178C:ssa ei ole myöskään ohjelmistotyökalujen sopivuuden tarkastelua [14], vaan se on siivottu DO-330:een [11].

## 2.4 DO-178:n turvallisuusluokat

Lentoteknisillä ohjelmistoilla on viisi epäonnistumisen luokkaa. Luokkien vaikutukset tutkitaan epäonnistumistilanteiden analysoinnilla. Epäonnistumista arvioidaan vaikutuksien mukaan. Sidosryhminä epäonnistumiselle ovat lentokone, lentohenkilöstö ja matkustajat. [10] Ohjelmistotasolla nämä suunnittelutakuutasot on määritelty SAE Internationalin julkaisemassa ARP4754A-dokumentin mukaisesti. [12] Jokaisen tason saavuttaminen vaatii edeltävän tasoon verraten moninkertaisen investoinnin. [14]

Lievin epäonnistuminen on tason E epäonnistuminen. E-luokan epäonnistuminen ei saa vaikuttaa turvallisuuteen, lentokaluston käyttöön tai edes lentohenkilöstön työmäärään. [10] E-luokkaa kuvataan turvallisuusvaikuttamattomaksi epäonnistumiseksi. [12]

Seuraavaksi lievin on luokan D epäonnistuminen. [10] Tätä kuvataan turvallisuusvaikutuksiltaan pieneksi. [12] Epäonnistuminen lisää hieman lentohenkilöstön työtä tai aiheuttaa turvallisuusmarginaalin pienentymistä vähäisesti. [10] D-luokan epäonnistuminen saattaa ilmentyä esimerkiksi lentosuunnitelmamuutoksena. [12]

Luokan C epäonnistuminen on taasen turvallisuusvaikutuksiltaan jo merkittävä. [12] Näissä tapauksissa lentohenkilöstön työmäärä lisääntyy huomattavasti tai turvallisuusmarginaalin pienentyminen on huomattavaa. [10] Merkittävä epäonnistuminen voisi olla esimerkiksi turbulenssista johtuva autopilotin liian nopea korjausliike, jonka matkustajat kokevat epämiellyttäväksi. [12]

B-luokan epäonnistuminen on turvallisuusvaikutuksiltaan vaarallinen [10, 12]. Epäonnistuminen ilmenee turvallisuuden alentumana tai vähentyneenä suorituskykynä. Suorituskyky voi laskea teknisten ongelmien vuoksi tai lentohenkilöstölle aiheutuvien ongelmien sekundäärivaikutuksena [10]. Esimerkki B-luokan epäonnistumisesta voisi

olla korkeusmittarin viallinen lukema, joka aiheuttaisi kovan laskeutumisen, jossa matkustajalle syntyisi vakava vamma tai jopa kuolema. [12]

Pahinta A-luokkaa [10] kutsutaan turvallisuusvaikutuksiltaan katastrofaaliseksi [12]. Epäonnistuminen saattaa aiheuttaa kuolemia ja usein koko ilma-aluksen menettämisen [10]. Esimerkki sulautetun järjestelmän ohjelmiston A-luokan epäonnistumisesta on Boeingin 737 Maxin ongelmat [15].

## 2.5 DO-178C:n vaatimukset

DO-178:ssa on tavoitteet jaettu kymmeneen taulukkoon. Taulukoissa on teemoittain aiheita. Taulukossa 1 nähtävissä on ohjelmistosuunnitteluprosessin vaatimukset DO-178C:ssä. Nämä vaatimukset koskevat ohjelmistotuotantoa. [12]

Taulukko 1: DO-178C A-1 [12]

| Sarja-numero | Tavoitteet | DAL-A | DAL-B | DAL-C | DAL-D |
|---|---|---|---|---|---|
| 1 | Ohjelmiston elinkaariprosessien toiminnot ovat määriteltyjä | X | X | X | X |
| 2 | Ohjelmiston elinkaaret, mukaanlukien prosessien väliset suhteet ja jaksotus, takaisinkytkennät ja muutoskriteerit ovat määriteltyjä | X | X | X | |
| 3 | Ohjelmiston elinkaaren ympäristö on valittu ja määritelty | X | X | X | |
| 4 | Muut näkökohdat ovat käsitelty | X | X | X | X |
| 5 | Ohjelmistotuotannon standardit ovat määriteltyjä | X | X | X | |
| 6 | Ohjelmisto vastaa suunnitelmatasolla DO-178:aa | X | X | X | |
| 7 | Ohjelmistokehitys- ja ohjelmistotarkistus suunnitelmat ovat koordinoituja | X | X | X | |

Ohjelmiston kehitysprosessiin liittyvät vaatimukset ovat taulukossa 2 [12]. Korkealla tasolla tarkoitetaan järjestelmävaatimuksien ja järjestelmäarkkitehtuurin analyysin pohjalta luotuja vaatimuksia. Matalan tason vaatimukset ovat ohjelmistovaatimuksia, joita vastaavaa lähdekoodia voi luoda ilman tarkempaa vaatimusmäärittelyä. [10] Korkean tason ja matalan tason vaatimukset sulautuvat, mikäli lähdekoodi tuotetaan korkean tason vaatimusten perusteella [12].

Taulukko 2: DO-178C A-2 [12]

| Sarja-numero | Tavoitteet | DAL-A | DAL-B | DAL-C | DAL-D |
|---|---|---|---|---|---|
| 1 | Korkean tason vaatimukset kehitetään | X | X | X | X |
| 2 | Johdetut korkean tason vaatimukset ovat määritelty ja luovutettu järjestelmäprosesseista vastaaville tahoille, mukaanlukien turvallisuuden arviointiprosessista vastaaville | X | X | X | X |
| 3 | Ohjelmistoarkkitehtuuri kehitetään | X | X | X | X |
| 4 | Matalan tason vaatimukset määritellään | X | X | X | |
| 5 | Johdetut matalan tason vaatimukset ovat määritelty ja luovutettu järjestelmäprosesseista vastaaville tahoille, mukaanlukien turvallisuuden arviointiprosessista vastaaville | X | X | X | |
| 6 | Lähdekoodi kehitetään | X | X | X | |
| 7 | Konekielinen suoritettavissa oleva koodi sekä parametritietotiedostot tuotetaan ja ladataan kohdetietokoneelle | X | X | X | X |

Taulukossa 3 on ohjelmistovaatimusprosessin tuotosten todentamiseen liittyvät tavoitteet [12].

Taulukko 3: DO-178C A-3 [12]

| Sarja-numero | Tavoitteet | DAL-A | DAL-B | DAL-C | DAL-D |
|---|---|---|---|---|---|
| 1 | Korkean tason vaatimukset vastaavat järjestelmän vaatimuksia | X | X | X | X |
| 2 | Korkean tason vaatimukset ovat täsmällisiä ja johdonmukaisia | X | X | X | X |
| 3 | Korkean tason vaatimukset ovat kohdetietokoneen kanssa yhteensopivia | X | X | | |
| 4 | Korkean tason vaatimukset ovat todennettavissa | X | X | X | |
| 5 | Korkean tason vaatimukset vastaavat standardeja | X | X | X | |
| 6 | Korkean tason vaatimukset ovat jäljitettävissä järjestelmän vaatimuksiin | X | X | X | X |
| 7 | Algoritmit ovat täsmällisiä | X | X | X | |

Taulukossa 4 on ohjelmistosuunnitteluprosessin tuotosten todentamisen tavoitteet. D-tason kriittisyydelle on vain yksi tavoite, joka sekin koskee osioituja ohjelmistoja. A- ja B-tason tavoitteiden määrä on sama. Näillä kriittisyyksillä matalan tason vaatimusten dokumentaatiolla on suuri painoarvo. [12]

Algoritmien täsmällisyys oli niin taulukossa 3 kuin taulukossa 4. Tällä tarkoitetaan syötteiden vasteen samankaltaisuutta. [12] Saman syötteen vasteen samankaltaisuuksissa saattaisi syntyä eroja esimerkiksi satunnaisuutta käytettäessä.

Taulukko 4: DO-178C A-4 [12]

| Sarja-numero | Tavoitteet | DAL-A | DAL-B | DAL-C | DAL-D |
|---|---|---|---|---|---|
| 1 | Matalan tason vaatimukset noudattavat korkean tason vaatimuksia | X | X | X | |
| 2 | Matalan tason vaatimukset ovat täsmällisiä ja johdonmukaisia | X | X | X | |
| 3 | Matalan tason vaatimukset ovat yhteensopivia kohdetietokoneen kanssa | X | X | | |
| 4 | Matalan tason vaatimukset ovat todennettavissa | X | X | | |
| 5 | Matalan tason vaatimukset vastaavat standardeja | X | X | X | |
| 6 | Matalan tason vaatimukset ovat jäljitettävissä korkean tason vaatimuksiin | X | X | X | |
| 7 | Algoritmit ovat täsmällisiä | X | X | X | |
| 8 | Ohjelmistoarkkitehtuuri on yhteensopiva korkean tason vaatimusten kanssa | X | X | X | |
| 9 | Ohjelmistoarkkitehtuuri on johdonmukainen | X | X | X | |
| 10 | Ohjelmistoarkkitehtuuri on yhteensopiva kohdetietokoneen kanssa | X | X | | |
| 11 | Ohjelmistoarkkitehtuuri on todennettavissa | X | X | | |
| 12 | Ohjelmistoarkkitehtuuri vastaa standardeja | X | X | X | |
| 13 | Ohjelmiston osioinnin eheys on varmistettu | X | X | X | X |

Nämä neljä ensimmäistä taulukkoa käsittelivät ohjelmistotuotannollisia vaatimuksia, jotka ovat voimassa ennen tuotantoa. Taulukot 5–9 käsittelevät tuotantoprosessin tavoitteita. Taulukossa 5 on ohjelmiston ohjelmoinnin ja integrointiprosessin tulosten todennuksen vaatimukset. Taulukossa 6 on integraatioprosessien tulosten varmentamisen tavoitteet. Taulukossa 7 on todentamisprosessin tulosten todentamisen tavoitteet. Taulukossa 8 on konfiguraationhallinnan prosessin tavoitteet. Taulukossa 9 on ohjelmiston laadunvarmistusprosessin tavoitteet. [12]

Taulukko 5: DO-178C A-5 [12]

| Sarja-numero | Tavoitteet | DAL-A | DAL-B | DAL-C | DAL-D |
|---|---|---|---|---|---|
| 1 | Ohjelmiston koodi noudattaa matalan tason vaatimuksia | X | X | X | |
| 2 | Lähdekoodi vastaa ohjelmistoarkkitehtuuria | X | X | X | |
| 3 | Lähdekoodi on todennettavissa | X | X | | |
| 4 | Lähdekoodi on standardien mukaista | X | X | X | |
| 5 | Lähdekoodi on jäljitettävissä matalan tason vaatimuksiin | X | X | X | |
| 6 | Lähdekoodi on tarkkaa ja johdonmukaista | X | X | X | |
| 7 | Ohjelmistointegraatioprosessin ulostulo on kokonainen ja oikein | X | X | X | |
| 8 | Parametritietojen tiedosto on oikein ja kokonainen | X | X | X | X |
| 9 | Parametritietojen tiedosto on verifioitu | X | X | X | |

Taulukko 6: DO-178C A-6 [12]

| Sarja-numero | Tavoitteet | DAL-A | DAL-B | DAL-C | DAL-D |
|---|---|---|---|---|---|
| 1 | Suoritettava konekielinen versio ohjelmasta täyttää korkean tason vaatimukset | X | X | X | X |
| 2 | Suoritettava konekielinen versio ohjelmasta on robusti suhteessa korkean tason vaatimuksiin | X | X | X | X |
| 3 | Suoritettava konekielinen versio ohjelmasta täyttää matalan tason vaatimukset | X | X | X | |
| 4 | Suoritettava konekielinen versio ohjelmasta on robusti suhteessa matalan tason vaatimuksiin | X | X | X | |
| 5 | Suoritettava konekielinen tiedosto on yhteensopiva kohdetietokoneen kanssa | X | X | X | X |

Taulukko 7: DO-178C A-7 [12]

| Sarja-numero | Tavoitteet | DAL-A | DAL-B | DAL-C | DAL-D |
|---|---|---|---|---|---|
| 1 | Testaamisen menettelytavat ovat oikeat | X | X | X | |
| 2 | Testaamisen tulokset antavat oikeita tuloksia ja poikkeamat ovat perustellut | X | X | X | |
| 3 | Testaaminen kattaa ohjelmistorakenteessa korkean tason ehdot | X | X | X | X |
| 4 | Testaaminen kattaa ohjelmistorakenteessa matalan tason ehdot | X | X | X | |
| 5 | Testaaminen kattaa ohjelmistorakenteessa muuttuneet ehdot ja päätökset | X | | | |
| 6 | Testaaminen kattaa ohjelmistorakenteessa päätöstenkäsittelyn | X | X | | |
| 7 | Testaaminen ohjelmistorakenteessa on lausekattava | X | X | X | |
| 8 | Testaaminen kattaa ohjelmistorakenteessa tieto- ja ohjauskytkennän | X | X | X | |
| 9 | Lähdekoodiin jäljittämättömissä olevan koodiston todennus | X | | | |

Taulukko 8: DO-178C A-8 [12]

| Sarja-numero | Tavoitteet | DAL-A | DAL-B | DAL-C | DAL-D |
|---|---|---|---|---|---|
| 1 | Määrityskohteet ovat tunnistettu | X | X | X | X |
| 2 | Lähtötasot ja jäljitettävyys ovat tunnettuja | X | X | X | X |
| 3 | Ongelmien raportointi, muutoksenhallinta sekä -tarkistus ja kokonaisuuden tilan hallinta ovat tunnettuja | X | X | X | X |
| 4 | Versionhallinta ja julkaisun hallinta ovat tunnettuja | X | X | X | X |
| 5 | Ohjelmiston kuormanhallinta on tunnettu | X | X | X | X |
| 6 | Ohjelmiston elinkaaren toimintaympäristönhallinta on tunnettu | X | X | X | X |

Taulukko 9: DO-178C A-9 [12]

| Sarja-numero | Tavoitteet | DAL-A | DAL-B | DAL-C | DAL-D |
|---|---|---|---|---|---|
| 1 | Varmuus ohjelmiston suunnitelmien ja standardien kehityksestä määräystenmukaisesti | X | X | X | |
| 2 | Varmuus ohjelmiston elinkaariprosessien sopivuudesta hyväksyttyyn ohjelmistosuunnitelmaan | X | X | X | X |
| 3 | Varmuus ohjelmiston elinkaariprosessien ohjelmistostandardiin sopimisesta | X | X | X | |
| 4 | Varmuus elinkaaren siirtymäprosessien kriteeristöstä | X | X | X | |
| 5 | Varmuus ohjelmiston määräyksienmukaisuuden varmistamisesta | X | X | X | X |

Taulukossa 10 on sertifiointiyhteysprosessin tavoitteet. Sertifiointiyhteysprosessin tavoitteet on sisällytetty taulukoihin väärinymmärrysten välttämiseksi, sekä selkeämmän viranomaisyhteistyön varmistamiseksi. [12]

Taulukko 10: DO-178C A-10 [12]

| Sarja-numero | Tavoitteet | DAL-A | DAL-B | DAL-C | DAL-D |
|---|---|---|---|---|---|
| 1 | Viestintä ja ymmärrys hyväksynnänhakijan sekä sertifioivan tahon välillä on olemassa | X | X | X | X |
| 2 | Vaatimuksenmukaisuuden keinot ovat esitetty ja suunnitelma määräystenmukaisuudesta on hankittu | X | X | X | X |
| 3 | Määräystenmukaisuuden perustelut ovat saatavilla | X | X | X | X |

Tavoitteet kattavat koko ohjelmiston elinkaaren viranomaisyhteistyöstä alkaen, suunnittelun kautta, päättyen koko sulautetun järjestelmän käytöstä poistoon. Tarkoituksena on luoda raamit onnistuneelle ohjelmistoprojektille, jossa panoksena on turvallisuus.

# 3. MIEHITTÄMÄTTÖMÄT ILMA-ALUKSET

## 3.1 Miehittämättömät ilma-alukset yleisesti

Miehittämätön ilma-alus, puhekielessä drooni tai drone [16], joskus UAV tai UAS, on lentämiseen tarkoitettu laite, jossa ei ole mukana ohjaajaa [3]. Miehittämättömiä ilma-aluksia voidaan ohjata kauko-ohjauksella, ne voivat lentää ennalta määrätyn reitin tai ne voivat olla autonomisia [2]. Kauko-ohjatut ilma-alukset ovat tällä hetkellä yleisin ilmentymismuoto [17].

Lennokki on käytössä harrastus- tai urheilutoiminnassa. Kaikki miehittämättömät ilma-alukset eivät siis ole lennokkeja, mutta kaikki lennokit ovat miehittämättömiä ilma-aluksia [17]. DO-178C koskee vain siviili-ilmailullisia toimijoita, jotka toimivat kaupallisesti [4].

Miehittämättömistä ilma-aluksista puhutaan usein niiden käytön kokonaisjärjestelmänä (eng. remotely piloted aircraft system), RPAS:ina. RPAS koostuu kauko-ohjatusta ilma-aluksesta (eng. remotely piloted aircraft), RPA:sta, sekä kauko-ohjauspaikasta (eng. remote pilot station), RPS:stä. Miehittämätöntä ilma-alusta ohjaa kauko-ohjaaja ja sen lennosta vastaa lennättäjä, ts. päällikkö, jonka lentotoiminnanharjoittaja on nimittänyt. Päällikkö ja kauko-ohjaaja voivat olla eri henkilöt. Usein lentotoimintaa avustaa kauko-ohjaustähystäjä, joka on lennättäjän hyväksymä henkilö, joka välittää aluksen tilasta ja lentoympäristöstä tietoa. [2]

## 3.2 Miehittämättömillä ilma-aluksilla tehtävä lentotoiminta

Kauko-ohjatuilla miehittämättömillä ilma-aluksilla voidaan lentää näköyhteyteen perustuen (eng. visual line-of-sight, VLOS). Tällöin kauko-ohjaajalla on apuvälineittä suora näköyhteys ilma-alukseen. Ilma-aluksesta tulevan videon perusteella lentäminen ei ole näköyhteyteen perustuvaa. [2]

Mikäli ilma-alusta ohjataan näköyhteydettä, voidaan tämä tehdä joko avustettuun ilmatilan tarkkailuun perustuen (eng. extended visual line-of-sight, E-VLOS) tai lentäen näköyhteyden ulkopuolella (eng. beyond visual line-of-sight, BVLOS). Avustetussa tarkkailussa toimitaan kauko-ohjaustähystäjän avulla. Kauko-ohjaustähystäjän tulee voida toimia ilman apuvälineitä. Näköyhteyden ulkopuolella toimittaessa lennetään apuvälineiden varassa ilman kauko-ohjaustähystäjää. [2]

Toiminnan laatu erottaa lentotyötoiminnan vaatimukset [17]. Koko EU:n alueella lentotoiminnanharjoittajilta vaaditaan tiukempia vaatimuksia, mikäli lentotyötoiminta ulottuu kauko-ohjaajan näköyhteyden ulkopuolelle [18]. Näköyhteyden ulkopuolella tapahtuvassa toiminnassa on usein myös monia ilmatilaan liittyviä vaatimuksia [2].

## 3.3 Miehittämättömät ilma-alukset Suomessa

Suomessa saa käyttää kameralla varustamattomia, alle 250 grammaisia lennokkeja ilman lupaa. Suomessa saa kuitenkin harrastemielessä lentää jopa 25 kg:n aluksilla. [18] Kaupallisessa toiminnassa painorajoja tai kamerallisuuteen liittyviä vaatimuksia ei ole, vaan kaikki toiminta on luvanvaraista [3].

Kauko-ohjattujen miehittämättömien ilma-alusten lentotyötä varten tarvitsee olla ajantasainen toimijailmoitus ja vastuuvakuutus. Lennoista tulee pitää kirjoja, joita tulee säilyttää ainakin kaksi vuotta. Ilma-aluksissa tulee olla vastuuhenkilön yhteystiedot. [17] Suomessa kauko-ohjattu miehittämätön ilma-alus, jota käytetään kaupallisessa toiminnassa, tarvitsee rekisteröidä ilma-alusrekisteriin, mikäli se painaa yli 150 kilogrammaa [19].

Suomessa on myös erillisiä vaatimuksia, mikäli lennätystoiminnassa toimitaan tiheästi asutuilla alueilla, lähellä väkijoukkoa, näköyhteyden ulkopuolella tai poikkeuksellisilla massoilla tai korkeuksilla. Poikkeuksellisissa lento-olosuhteissa vaaditaan toimintatapoja tai teknisiä ratkaisuja, jotka takaavat aluksen turvallisen alas saaton. BVLOS-toiminnassa tarvitsee Suomessa tehdä toimintakuvaus, turvallisuusarviointi ja toimintaohjeistus, mitkä tulee toimittaa Traficomille. Traficom luo aktivoitavan tilapäisen vaara-alueen ilmatilaan. [17]

Traficomin mukaan Suomessa oli vuoden 2020 alussa 2962 lentotyöluvallista UAS-toimijaa. Heillä oli rekisteröitynä vajaa 4000 ilma-alusta. Tämän lisäksi lisensioimattomia harrastajia arvellaan olevan noin 50000. [20]

## 3.4 Miehittämättömät ilma-alukset EU:ssa

EU:n alueella vuodesta 2021 alkaen kaikkien yli 250 grammaisten ja kaikkien kamerallisten dronejen käyttäjien tulee rekisteröityä. EU:n dronesäännöt jakavat lentämisen avoimeen, erityiseen sekä sertifioituun kategoriaan. [18] Rajoitteiden lisäksi toimijoille tulee mahdollisuus toimia paljon laajemmalla toimialueella [20].

EU:n droneasetuksessa avoimen kategorian toiminta on alle 120:ssä metrissä näköyhteyden alaisesti tapahtuva lentotoiminta alle 25 kg:n droneilla. Avoin luokka jaetaan erikseen luokkiin A1, A2 ja A3. [18] Mikäli toiminta on avoimen luokan toimintaa vaarallisempaa, tarvitsee kauko-ohjaajan olla hyväksytty erityisen kategorian toimintaan. Mikäli kyseessä on operaatio, joka on todella riskialtis, tarvitsee kauko-ohjaajan sekä ilma-aluksen olla hyväksyttyjä sertifioituun kategoriaan. [21]

EU:n droneasetus asettaa ilma-aluksille erityisiä teknisiä vaatimuksia riippuen toiminnan riskeistä [20]. EU:n droneasetus koskee Suomessa lähinnä harrastajia, sillä harrastetoiminta ei ollut Suomessa kovin säädeltyä. Droneasetus tulee lisäämään etenkin laitteiston ohjelmistopuolen vaatimuksia. [18] Huomattavaa on, että jo näköyhteyden ulkopuolella toimiminen vaatii erityisen kategorian pätevyyden [20].

## 3.5 Miehittämättömät ilma-alukset Yhdysvalloissa

Yhdysvalloissa harrastajille dronetoiminta on kutakuinkin EU:n avoimen luokan mukaista. Lisensiointia vaaditaan yli 250 grammaisilta aluksilta, suurin sallittu massa on 55 paunaa (~24,95 kilogrammaa), suurin sallittu lentokorkeus on alle 400 jalkaa (121,92 metriä), toiminnan on oltava G-luokan ilmatilassa sekä toimintaa tulee harrastaa vain huvin vuoksi. [22]

Yhdysvalloissa lentoviranomainen ei aseta kaupallisille toimijoille suuria vaatimuksia. Käytännössä lentää saa testin läpäistyään rekisteröidyllä ilma-aluksella. Ilma-alukseen pätee samat ehdot kuin harrastelennokkeihin. Painorajat ylittävä toiminta vaatii paikalliselta yhdistykseltä oikeutuksen. [23] Yhdysvalloissa opetustoiminta ei ole ammatillisen toiminnan sääntelyn piirissä [24], toisin kuin EU:ssa [21].

# 4. MIEHITTÄMÄTTÖMIEN ILMA-ALUSTEN DO-178C:N NOUDATTAMINEN

## 4.1 Lainsäädännön ja valvonnan nykytilanne

Tähän mennessä Yhdysvaltojen lentoviranomainen ei ole vaatinut kaupallista toimintaa harrastavilta miehittämättömiltä ilma-aluksilta DO-178C:n mukaista ohjelmistoa [25]. Euroopan lentoturvallisuusvirastolla taasen ei ole ollut yhteisiä ohjenuoria miehittämättömien ilma-alusten ohjelmistoihin liittyen. [20] Yhdysvallat sekä EU ovat alkaneet luomaan jyrkempää säätelyä myös miehittämättömään lentokalustoon liittyen [18, 20, 25].

Yhdysvalloissa ARP4754:n noudattamista on katsottu siitä näkökulmasta, että SAE:n standardi tarkastelee ilma-aluskohtaisesti turvallisuutta. 2020-luvun puolivälissä tulevassa kaupallista toimintaa miehittämättömillä ilma-aluksilla säätelevässä ohjeistuksessa aluksille tulee olemaan teknisiä vaatimuksia liittyen etätunnistukseen. Säätelyä tulee myös liittyen toimintaan muissakin ilmatiloissa, kuin tyhjissä, G-luokasta poikkeavissa ilmatiloissa. [25]

Euroopan lentoturvallisuusvirasto on myös työskennellyt tuottaakseen sertifioidun kategorian sääntöjä. Tällä hetkellä säännöstö liityen niin kalustoon kuin lentävään tahoon ovat valmistelussa. Euroopassa ilmatilarajoituksista päättää kansallinen säätely. [20]

Niin Yhdysvaltojen lentoviranomainen kuin Euroopan lentoturvallisuusvirasto ovat siis muuttamassa lentokaluston teknisiin vaatimuksiin liittyviä vaatimuksia. ARP4754:sta ollaan poikkeamassa, sillä vikasietotasoa aletaan määrittämään laajennetusti muihin toimijoihin samassa ilmatilassa. Tämä muuttaa dynamiikkaa, kun vaikutusten arvionti laajenee alusten väliseksi.

## 4.2 Vaaditun vikasietotason määrittely

Analysoidessa, miten ilma-alus voisi vaikuttaa toisiin ilmatilassa toimiviin täytyy miettiä skenaarioita, joihin saatettaisiin päätyä ja tilanteita, joihin on jo päädytty. Pahimmassa tapauksessa ilma-alukset saattaisivat törmätä ja tämä saattaisi aiheuttaa jopa lentokoneen menetyksen ja ihmisuhreja. Alueella huolimattomasti toimiminen on jo nyt aiheuttanut korjausliikkeitä ja törmäyksen – ilman mittavaa vahinkoa [26]. Väärän luokan ilmatilassa toimiminen on aiheuttanut lentosuunnitelmiin muutoksia [27]. Lievimmässä tapauksessa turvallisuusvaikutus jää oikeutetun toimijan pään pudistukseksi.

Miehitettyjä lentokoneita testataan törmäyksiä vastaan. Vuoden 2017 heinäkuun jälkeen lentokonevalmistajat ovat joutuneet tekemään lintutestejä erisuuruisilla nopeuksilla. Käytännössä matkustajalentokoneen peräsimen pitää kestää vajaan neljän kilon ja muiden osien, mukaan lukien moottorin, tulee kestää vajaan kahden kilon linnun osuma 370:n ja 450:n kilometrin tuntinopeudella. [28] Luonnollisten ja synteettisten materiaalien suoranainen vertailu tässä tapauksessa ei ole suoraviivaista. Synteettisillä materiaaleilla, joita miehittämättömissä ilma-aluksissa käytetään, on

suhteessa parempi jännitettä kestävä voima, kun taasen puristusvoimien vastustuskyky ei ole varsin suuri [29]. Materiaalien hajoamistapa siis eroaa, mutta olettaen pahimman tapauksen täysin elastisen törmäyksen, on rakenteet testattu kuitenkin massoiltaan vastaavien törmäysten osalta [28]. Raskaimpien miehittämättömien ilma-alusten kohdalla siis voidaan todeta katastrofaalisen epäonnistumisen riskin olevan olemassa.

Huomattavasti todennäköisempi skenaario on väärässä ilmatilassa toimiminen tai oikeutetussa ilmatilassa väärin toimiminen. Tämä aiheuttaa turvallisuusvaikutuksiltaan pieniä riskejä [10]. Todennäköinen syntyvä muutos on lentoreittimuutos [12]. Tämä riski on olemassa kaikilla miehittämättömillä ilma-aluksilla. Riskin realisoitumista edesauttaa suunniteltu transponderipakko [25].

Miehittämättömät ilma-alukset siis hyötyisivät suuresti valvonnan muutoksen näkökulmasta, mikäli ne täyttäisivät edes tason D vaatimukset. Tällä tasolla toimimalla kyettäisiin estämään suurin osa nykyisin yleisistä lentosuunnitelman muutoksista. Yli 25 kg aluksien kanssa korkeamman tason vaatimukset tulevat ajankohtaisiksi.

## 4.3 Saavutettavat hyödyt DO-178C:llä

Standardin seuraamisen suurimmat hyödyt ovat elinkaarenhallintaa pohtiessa etukäteisvaatimusten selkeydessä. Vaatimusten selkeys edesauttaa myös iteraatioiden vähentämisessä. Iteraatioiden vähyys vähentää tuotannossa ja käytössä olevan kaluston heterogeenisyyttä, joten virheenhallinta on helpompaa. [30]

Käytännön kilpailuetua standardin seuraamisesta saa sillä, että lähes kaikki kansainväliset toimijat tunnustavat DO-178C:n. Yhden standardin täyttämällä on siis pääsy lähes kaikille markkinoille [14]. Niin taloudellista, kuin maineellista säästöä syntyy myös sitä kautta, että tuotantoon ei pääse täyttämättä standardeja. Tämä vähentää todella kalliita kentällä löytyviä virheitä.

Selkeämmät käyttö- ja testaustapauskuvaukset vähentävät bugien löytymistä moduulitestivaiheissa. Testaaminen standardin mukaisesti tuo myös testaukseen lisää kattavuutta ja perinteisiä limittäisyyksien huomioimattomuuksia ei pääse syntymään. [30] Selkeys parantaa laadun varmistusta laadunvarmistusdokumenttien, ohjelmiston sopivuustestien ja ohjelmiston aikaansaannostiivistelmän kautta [14].

Kansainvälisen standardin seuraamisesta syntyy myös hyöty henkilöhallinnon tasolla. Hajanaisen osaamiskentän sijaan olisi mahdollista, että työvoimalla koko ilmailualalla olisi hyvä liikkuvuus. Tämä lisäisi miehittämättömien ilma-alusten ohjelmisto-osaajien joukkoon ison osan jo tällä hetkellä ilma-alusten parissa työskentelevistä.

## 4.4 DO-178C:n tavoitteiden soveltuvuuden arviointi

Kappaleessa 2.5 esiteltiin DO-178C:n vaatimukset. Kappaleessa 4.2 tunnistettiin DAL-D:n mukaisiin tavoitteisiin vastaamisen yleisesti miehittämättömille ilma-aluksille hyväksi tasoksi. Tässä kappaleessa tarkastellaan, soveltuuko DO-178C:n vaatimukset miehittämättömien ilma-alusten käyttöön huomioiden alusten erityislaatuisuuden.

Ensimmäisen taulukon *muiden näkökohtien huomioiminen* on varsin dynaaminen prosessi, sillä muutospaineita valvovilta tahoilta saattaa syntyä lyhyelläkin aikataululla [20, 25]. Samaisen kohdan joutuisi myös huomioimaan jo D-tason kriittisyydellä.

Taulukossa 2 huomattavaa on suljetun lähdekoodin ulkoa ostamisen mahdollisuus D-tasolla. Tällöin esimerkiksi olisi mahdollista ostaa osajärjestelmiä, kuten

kameramoduuleita, toimittajilta, joilla on runsaasti kaupallisia intressejä pitää ohjelmisto-osaaminen talonsa sisällä.

Taulukossa 3 on ohjelmistovaatimusprosessin tuotosten todentamiseen liittyvät tavoitteet. Myös vaatimusprosessi antaa varsin kevyet raamit toimijoille, jotka tarvitsevat vain D-tason kriittisyydellistä ohjelmistoa. Vaatimusprosessi antaa myös samaisille toimijoille mahdollisuuden muuntaa laitteistoa kesken ohjelmiston elinkaaren ilman erillistä auditointia.

Taulukossa 4 D-tason kriittisyydelle on vain yksi tavoite, joka sekin koskee osioituja ohjelmistoja. A- ja B-tason tavoitteiden määrä on sama. Näillä kriittisyyksillä matalan tason vaatimusten dokumentaatiolla on suuri painoarvo.

Taulukoissa 5 ja 6 ohjelmoinnin ja integroinnin vaatimukset soveltuvat hyvin miehittämättömien ilma-alusten käyttöön. Taulukoiden tavoitteita seuraamalla pääsee varsin robustiin sulautetun järjestelmän integraatioon. Tavoitteet myös antavat mahdollisuuden muuttaa kohdetietokonetta niin, että järjestelmäintegraatiosta vain osia on varmistettava.

Taulukon 7 testaamistavoitteet täyttämällä ilmailukriittisiä osia ei jää testaamatta. Testaamiseen liittyvät tavoitteet skaalautuvat varsin vahvasti kriittisyydestä riippuen. Tämä antaa mukautumisvaraa, mikäli olisi tarkoituksenmukaista siirtyä kriittisyysluokissa ylöspäin.

Taulukot 8 ja 9 ovat varsin anteeksiantamattomia riippumatta tasosta. Konfiguraationhallinnan sekä laadunvarmistusprosessin tavoitteiden täyttäminen kuitenkin edesauttavat ilmailukriittisen ohjelmistotuotannon kanssa. Nämä tavoitteet saattavat olla haasteellisia ketteriin menetelmiin tottuneille yrityksille.

Taulukon 10 tavoitteet täyttämällä yritys varmistuu oman toimintansa soveltuvuudesta tehtävään. Tavoitteiden täyttäminen täytyy, kun aluksen ilmakelpoisuutta varmistetaan viranomaisten toimesta.

Etenkin DAL-D-tasolla toimiville toimijoille vaatimukset antavat varsin paljon harkinnanvaraisuutta monien osakokonaisuuksien osalta. Oman toiminnan erikoislaatuisuuden huomioiminen on mahdollista. Kaikkia kappaleessa 2.5 esiteltyjä vaatimuksia voitaisiin pitää soveltuvina myös miehittämättömille ilma-aluksille.

## 4.5 DO-178:n haasteet miehittämättömiä ilma-aluksia tuottaville tahoille

Laitteistoon liittyvää sääntelyä on tulossa yli 25 kilogramman aluksille. [21, 23] Euroopan unionissa kuitenkin on jätetty alle 150 kiloiset ilma-alukset kansallisen sääntelyn ja valvonnan piiriin. [19] On siis mahdollista, että varianssia tulkintojen sekä Euroopan lentoturvallisuusviraston säännöstön toimeenpanon suhteen tulee olemaan kansallisella tasolla. Tällä on lähinnä vaikutusta tulkittuun vikasietotasoon ja sitä kautta ARP4754:stä saataviin tavoitteisiin.

Standardiin siirtyminen tuottaa yritykselle lisätyötä. Haastavaa on muuntaa työtapoja ja täsmällisyyden, jäljitettävyyden sekä tiedottamisen tasojen muuttaminen. [14] Myöskin työntekijäpoolin osaamista on vaikea kartuttaa koulutusmahdollisuuksien vähyyden vuoksi. On olemassa varsin vähän formaalia koulutusta järjestelmä- ja ohjelmistovalidointia sekä -varmistamista varten. [12]

Työntekijöiden koulutuksen lisäksi työvoimaan liittyy järjestelyn ja hankkimisen ongelmia. Kokeneiden turvallisuusinsinöörien, jotka ovat kasvaneet ammattilaisina läpi ilmailualan turvallisuusstandardien muutoksen, pooli on vähenemään päin. Näiden ammattilaisten kanssa poistuu ymmärrys kokonaiskuvasta, ja siitä miksi standardit ovat kehittyneet nykyisenlaisiksi. Työvoiman laadun vuoksi osajärjestelmien ulkoistus on varsin houkutteleva vaihtoehto, mutta vaarana on, että ulkoistettu taho ei ymmärrä täysin kyseisen järjestelmän erityislaatuisuutta [12].

DO-178C:hen liittyy oleellisesti DO-330, joka määrittelee ohjelmistotyökalujen sopivuuden. Ilma-alukseen ohjelmistoja tuottavan tahon tarvitsee analysoida omien työkalujensa sopivuutta ja sovittaa ne yhteensopiviksi DO-330:n kanssa [12]. Tämä tuottaa työntekijöiden koulutustarvetta.

## 4.6 DO-178C:n kustannukset tuottaville tahoille

DO-178B:stä DO-178C:hen siirtymisestä syntyvät kustannukset ovat varsin hyvin dokumentoituja [14, 30]. Siirtymästä syntyvät kustannukset tulevat suurina lähinnä tahoille, joilla DO-178B:n seuraamisessa ollaan laadunhallinnassa sekä dokumentoinnissa menty vain standardin minimitasolla ja vikasietotaso on ollut korkea [14]. DO-178B:n seuraaminen lisäsi ohjelmistoprojektin kustannuksia noin 20—40 %, riippuen kriittisyydestä [30]. DO-178C on suhteessa noin 25—40 % kalliimpi [14]. Nämä luvut ovat ilmailuteollisuudesta, jossa henkilöstöllä sekä yrityksillä on osaaminen ja kokemus standardeista. Suurimmat kustannukset tulevat siis DO-178-ekosysteemiin siirtymisestä, ei niinkään liikkuvuudesta standardien välillä.

Kustannuksia syntyy myös jo aiemmin kappaleessa 4.5 mainitun työvoimalle syntyvän koulutustarpeen vuoksi. Työntekijät ja organisaatio joutuvat mukautumaan uuteen tuotantoympäristöön, sekä työkalustoon. Molemmat synnyttävät kustannuksia joko suoraan tai välillisesti tuottavuuden laskiessa suhteessa käytettyyn työaikaan.

Taulukko 11: Viansietotasojen suhteelliset kustannukset sekä tavoitteiden määrä

| Viansietotaso | Suhteellinen kustannus [14] | Tavoitteet (kokonaislukumäärä) [12] | Tavoitteet, joiden tulee toteutua itsenäisesti [12] |
|---|---|---|---|
| DAL-A | 10 | 71 | 30 |
| DAL-B | 9 | 69 | 18 |
| DAL-C | 5 | 62 | 5 |
| DAL-D | 3 | 26 | 2 |
| DAL-E | 1 | 0 | 0 |

Taulukosta 11 nähdään, että kustannushyppy on suurin nimenomaan siirryttäessä vaatimustasolta D ylöspäin. Tasolta B tasolle A siirtyminen ei synnytä suurta suhteellista kustannusta. Tavoitteiden kokonaismäärä ei nouse ylemmillä tasoilla yhtä paljon suhteellisesti, vaan lähinnä itsenäisesti toteutuvien tavoitteiden määrässä on suuri muutos. Kustannuksien valossa siis optimaaliset saavutettavat tasot ovat DAL-D sekä DAL-A.

# 5. YHTEENVETO

Työssä tarkasteltiin ensin ilmailuun liittyviä turvakriittisiä järjestelmiä sekä niihin liittyviä standardeja. Ilmailualaan liittyvän nykyisen standardoinnin ymmärtäminen on tärkeää antamaan kontekstia vaatimuksille, jotka ovat syntymässä laillisissa prosesseissa. Standardien ymmärtäminen on myös tärkeää, koska niitä hyödyntämällä pääsee toimintaympäristössä sopivaksi todettuihin tavoitteisiin ilman tarvehankintamaista kokoamisprosessia ja pitkäaikaista iteraatiota.

Nykystandardien jälkeen työssä tutustuttiin siihen, miten miehittämättömät ilma-alukset ja niillä tehtävä toiminta luokitellaan. Ilmailuala on globaalisti varsin yhtenäinen, ja tarkastelu tässä työssä keskittyi kahden suurimman valvovan organisaation maantieteellisille alueille, eli Yhdysvaltoihin sekä Euroopan Unioniin. Suurinta varianssia alalla on kaupallisen toiminnan erottamisessa muusta toiminnasta.

Lopuksi työssä arvioitiin sertifioinnin nykytilaa ja DO-178C:n soveltuvuutta. Kenttä on tällä hetkellä varsin hajanainen, mutta ilmailuturvallisuusorganisaatiot ovat vastaamassa muutoksiin. Miehittämättömät ilma-alukset hyötyisivät muutosprosesseissa ilmoitettujen tavoitteiden valossa hyötyvän suuresti sekä varsin kustannustehokkaasti DAL-D-tason DO-178C:n tavoitteiden täyttämisestä.

Aihe on ajankohtainen, sillä lainsäädännössä sekä valvonnassa on aloitettu suuria muutosprosesseja, joihin teollisuuden tulee vastata. Vaaratilanteita ja vahinkoja on päässyt jo tapahtumaan, käyttäjäjoukkojen määrä on alati kasvava ja käyttökohteita tulee huomattavasti lisää kaupalliselle puolelle. Kaupallinen ilmailutoiminta on varsin säädeltyä ja asiakassegmentti kantaa paljon vastuuta. Tuottavien tahojen tulee kyetä tarjoamaan turvallisia ja soveltuvia ratkaisuja muuttuvalla toimialalla.

Työn havaintojen perusteella vaikuttaa, että toimijoiden kannattaisi omaksua DO-178C. Standardin luomat hyödyt peittoavat kustannukset pitkällä aikavälillä. Omaksuminen laajentaa huomattavasti palkattavien työntekijöiden poolia, varmistaa pääsyn jatkossakin kaikille markkinoille sekä DAL-D-tason täyttämällä edesautettaisiin huomattavasti ilmailuturvallisuuden parantamista. Standardin täyttämällä myös tulevaisuuden sääntömuutoksiin mukautuminen tulee olemaan halvempaa ja mahdollisesti hyvin erityislaatuisten tuotteiden kohdalla kovien vaatimustasojen täyttäminen olisi huomattavasti edullisempaa, kuin tuotekohtaisen hyväksynnän hakeminen.

# LÄHTEET


[1] Grand View Research (2019), *Commercial Drone Market Size, Share & Trends Analysis Report By Application (Filming & Photography, Inspection & Maintenance), By Product (Fixed-wing, Rotary Blade Hybrid), By End Use, And Segment Forecasts, 2019 – 2025*

[2] Traficom (2020), *OPS M1-32, Kauko-ohjatun ilma-aluksen ja lennokin käyttäminen ilmailuun,* TRAFICOM/42450/03.04.00.00/2020

[3] Ilmailulaki 864/2014

[4] U.S. Department of Transportation, Federal Aviation Administration (2013.), *Airborne Software Assurance*, saatavilla: https://web.archive.org/web/20140903075843/http://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_20-115C.pdf, luettu 14.03.2021

[5] Sommerville, I. (2011), *Software engineering,* 10. ed.

[6] Firesmith, D. (2017), *Engineering Safety- and Security-Related Requirements for Software-Intensive Systems*, saatavilla: http://resources.sei.cmu.edu/asset_files/Presentation/2010_017_001_23266.pdf, luettu: 19.03.2021

[7] Bowen, J., Stavridou, V. (1993), *Safety-critical systems, formal methods and standards*

[8] Goble, W. (2010), *Control Systems Safety Evaluation and Reliability,* 3. ed

[9] International Organisation for Standardization (2018), ISO 26262-1:2018(en), saatavilla: *https://www.iso.org/obp/ui/#iso:std:iso:26262:-1:ed-2:v1:en*, luettu 23.03.2021

[10] Rapita Systems (2021.), *DO-178C Guidance*, saatavilla: https://www.rapitasystems.com/do178c-testing, luettu 14.03.2021

[11] U.S. Department of Transportation, Federal Aviation Administration (2013.), AC 20-115C, saatavilla: https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_20-115C.pdf, luettu 14.03.2021

[12] Rierson, L. (2013), *Developing Safety-Critical Software: A Practical Guide for Aviation Software and DO-178C Compliance*

[13] RTCA Inc. (2011), *RTCA/DO-178C Software Considerations in Airborne Systems and Equipment Certification*

[14] IBM Software (2014), *DO-178C compliance: turn an overhead expense into a competitive advantage*

[15] Campbell, D. & Joel W. (2019), *Redline: The many human errors that brought down the Boeing 737 Max*, saatavilla: https://www.theverge.com/2019/5/2/18518176/boeing-737-max-crash-problems-human-error-mcas-faa, luettu 23.03.2021

[16] Kielikello (2018), *Drone vai drooni?*, saatavilla: https://www.kielikello.fi/-/drone-vai-drooni-, luettu 27.03.2021

[17] Droneinfo (2021), *Lentotyö*, saatavilla: https://droneinfo.fi/fi/droneja-kayttavat-ammattilaiset, luettu 27.03.2021

[18] Droneinfo (2021), *EU:n Dronesäännöt*, saatavilla: https://droneinfo.fi/fi/eun-dronesaannot, luettu 27.03.2021

[19] Eduskunta (2017), *Hallituksen esitys HE145/2017 vp*, saatavilla: https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_145+2017.aspx, luettu: 29.03.2021

[20] Traficom (2020), *Drone-infotilaisuus 30.1.2020*, saatavilla: https://www.traficom.fi/fi/tilastot-ja-julkaisut/tilaisuudet/drone-infotilaisuus-3012020, luettu: 29.03.2021

[21] EASA (2019), *Easy Access Rules for Unmanned Aircraft Systems (Regulation (EU) 2019/947 and Regulation (EU) 2019/945)*

[22] U.S. Department of Transportation, Federal Aviation Administration (2021), *Recreational Flyers & Modeler Community-Based Organizations*, saatavilla: https://www.faa.gov/uas/recreational_fliers/, luettu: 30.03.2021

[23] U.S. Department of Transportation, Federal Aviation Administration (2021), *Certificated Remote Pilots including Commercial Operators*, saatavilla: https://www.faa.gov/uas/commercial_operators/, luettu: 30.03.2021

[24] U.S. Department of Transportation, Federal Aviation Administration (2021), *Educational Users*, saatavilla: https://www.faa.gov/uas/educational_users/, luettu: 30.03.2021

[25] Careless, J. (2020), *Will the FAA Establish a New Commercial Drone Avionics Mandate?*, saatavilla: http://interactive.aviationtoday.com/avionics-magazine/april-may-2020/will-the-faa-establish-a-new-commercial-drone-avionics-mandate/, luettu: 31.03.2021

[26] BBC News (2017), *Drone collides with commercial aeroplane in Canada*, saatavilla: https://www.bbc.com/news/technology-41635518, luettu: 01.04.2021

[27] BBC News (2020), *'Kill switch' failed as drone hit controlled space near Gatwick*, saatavilla: https://www.bbc.com/news/uk-england-sussex-56112694, luettu: 01.04.2021

[28] Trimble, S. (2018), *Regulators propose new rule for engine bird ingestion*, saatavilla: https://www.flightglobal.com/systems-and-interiors/regulators-propose-new-rule-for-engine-bird-ingestion/128729.article, luettu 01.04.2021

[29] Ueda, M., Hiraga, A., Nishimura, T. (2011), *Compressive Strength of a Carbon Fiber in Matrix*

[30] Hilderman, V. (2014), *DO-178C Costs Versus Benefits*, saatavilla: https://afuzion.com/do-178c-costs-versus-benefits/, luettu: 01.04.2021