Veilig Ontwerp van Intelligente Transportsystemen

Rick R. Feith and E. van Kampen
TU Delft, Postbus 5058, 2600GB Delft, Nederland

"Safe-by-Design vraagt om een andere mindset, die gericht is op interdisciplinaire samenwerking en op veiligheid als belangrijke voorwaarde voor technologisch ontwerp[*]". De gevolgen van het toepassen van nieuwe ontwikkelingen hebben soms onbedoelde implicaties die lastig te overzien zijn. Risico's voor mens en milieu kunnen beter voorkomen worden door deze al in de ontwerpfase mee te nemen. Dit vraagt om een (nieuwe) veiligheidscultuur voor onderzoekers, productontwikkelaars en management. Deze veiligheidscultuur verkleint ook de kans op problemen in een later stadium waar eventuele gevolgen veel groter kunnen zijn. Een interdisciplinaire samenwerking en uitwisseling van kennis kan de product veiligheid en duurzaamheid vergroten. In opdracht van het Ministerie van Infrastructuur en Waterstaat wordt in deze studie de luchtvaartsector bekeken. Als voorbeeld van een interdisciplinaire samenwerking wordt hier de levenscyclus van een vliegtuig beschreven, vervolgens wordt Safe-by-Design op het gebied van intelligente systemen toegelicht. Waardevolle tools met betrekking tot algemene veiligheid worden uitgelicht en kunnen ook een bijdrage leveren aan andere sectoren.

I. Introductie

Transportsystemen worden steeds zelfstandiger en intelligenter. Dit zien we op de weg in de vorm van zelf-rijdende auto's [1], op het spoor met autonome treinen, en ook in de luchtvaart met een stijging van het aantal onbemande vluchten van drones (UAV's)[†] en autonome Personal Air Vehicle (PAV's). Deze ontwikkeling roept veel nieuwe vragen op wat betreft de veiligheid van deze systemen, bijvoorbeeld rondom autonome besluitvorming en mens-machine interacties.

Het samenbrengen van verschillende disciplines kan tot innovatieve oplossingen leiden. Een voorbeeld is de samenwerking van de biologie, computer techniek en luchtvaart techniek, wat heeft geleid tot de toepassing van "reinforcement learning[‡]" op flight control systemen van vliegtuigen [2, 3]. Het toepassen van meerdere disciplines in een ontwerp zoals gebeurt bij autonome systemen kan leiden tot onbedoelde gevolgen. Het toepassen van Safe-by-Design principes kan dan nuttig zijn om eventuele latere problemen te voorkomen.

Dit literatuuronderzoek wordt uitgevoerd in opdracht van het Ministerie van Infrastructuur en Waterstaat en bestaat uit twee delen. Ten eerste wordt gekeken hoe specialisten uit verschillende disciplines in een interdisciplinair project nadenken over de veiligheid tijdens de ontwerpfase voor de discipline waar zij zich mee bezighouden en welke impact dit heeft op de totale veiligheid, duurzaamheid en levenscyclus van het totale eindproduct. Dit zal worden gedaan aan de hand van de luchtvaartsector, waar de operationele veiligheid al jaren hoog is. Ook zal er een case-study plaats vinden van de recente Boeing 737-8 MAX problematiek om het belang van Safe-by-Design te onderbouwen.

Ten tweede wordt gekeken naar de operationele veiligheid van een specifiek intelligent systeem met als doel om een veiligheidsbewustzijn bij ontwikkelaars te creëren. Omdat de innovatie vaak voorloopt op de regelgeving is deze bewustwording bij ontwikkelaars van groot belang. Om dit te onderzoeken zal worden gekeken naar reinforcement learning toegepast op flight control systemen van vliegtuigen. Hiervoor wordt als eerste kort uitgelegd hoe veiligheid gedefinieerd is, ten tweede wordt gekeken naar de benodigde informatie om veiligheid van het totale systeem te garanderen. Tot slot wordt gekeken hoe de veiligheid gewaarborgd blijft tijdens de leerfase van reinforcement learning. Een Safe-by-Design intelligent systeem is hier van groot belang omdat tijdens de leerfase vaak willekeurige acties worden uitgevoerd en daardoor de onzekerheid van de prestatie zeer hoog is.

[*] https://www.safe-by-design-nl.nl/default.aspx

[†] https://www.ilent.nl/onderwerpen/luchtvaartuigregister/documenten/publicaties/2019/05/27/luchtvaartuigregister-aircraft-registration

[‡] Een zelflerende methode welke leert aan de hand van in het verleden gemaakte beslissingen

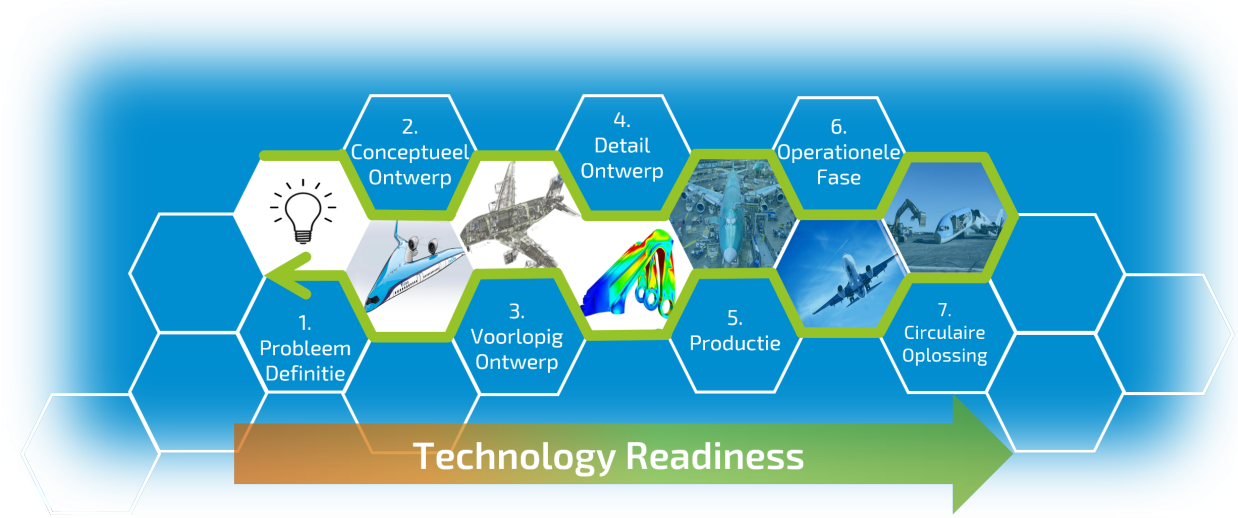

Fig. 1 Complete levensloop van een vliegtuig.

II. Multidisciplinair Design

Het ontwerpen en bouwen van een vliegtuig bevat tientallen verschillende disciplines, elk met eigen uitdagingen en voorschriften. Om tot een volledig overzicht te komen zal de totale levensloop van een vliegtuig geïdentificeerd worden. Daarbij wordt in kaart gebracht welke disciplines meewerken in elke fase, welke risico's er optreden en hoe daar op wordt geanticipeerd tijdens de ontwerpfase. In vergelijking met andere sectoren is de luchtvaartsector onderhevig aan strenge regelgeving [4] wat bijdraagt aan de operationele veiligheid. Ook is een veiligheidsbewustzijn al geruime tijd een belangrijk onderdeel van de luchtvaart[§]. Safe-by-Design gaat verder dan alleen de operationele veiligheid, daarom wordt er ook gekeken hoe wordt nagedacht over de duurzaamheid en veiligheid tijdens de gehele levenscyclus van het vliegtuig. In deze sectie wordt ten eerste de levensloop van een vliegtuig bestudeerd. Vervolgens wordt de case-study van de Boeing 737-8 MAX gepresenteerd.

A. Totale Levensloop

Het ontwerpen, bouwen, testen en certificeren van een nieuw vliegtuigontwerp is een proces dat tot 10 jaar in beslag kan nemen [5] en enorme investeringen vraagt. De totale levensloop wordt gevisualiseerd in figuur 1. Deze wordt hieronder uitgelegd.

1. Probleem Omschrijving

Gezien de doorlooptijd en kosten die verbonden zijn aan het ontwerpen van een nieuw model, lopen vliegtuigfabrikanten een groot financieel risico. De investering in een nieuw ontwerp vereist kapitaal en de terugverdienperiode is lang, de toekomst van het bedrijf staat letterlijk op het spel [5, 6], een safe-by-design investering denken (gericht op de toekomst) is dan van belang om eventuele desinvesteringen, aansprakelijkstelling en imagoschade te voorkomen. Figuur 2 laat zien hoe een relatief korte project-ontwerp-periode het succes van de investering bepaalt. Daarom begint het ontwerp met een probleemomschrijving. Dit vereist een lange termijn denken waarbij een uitgebreide marktanalyse en risicoanalyse worden uitgevoerd. Ook wordt uitgebreid gekeken naar toekomstige trends wat betreft wetgeving en milieueisen. Tot slot wil een ontwerper innoveren om aantrekkelijker te worden voor kopers, hierbij wordt gedacht aan het terugdringen van kosten door bijvoorbeeld het brandstofverbruik te verlagen. Ook kunnen unieke "sellingpoints" ontworpen worden, zo heeft bijvoorbeeld Airbus met de A380 destijds het geluid in de cabine significant weten terug te dringen om het comfort voor passagiers te verhogen[¶]. Uiteindelijk resulteert deze fase in de ontwerpvoorwaarden.

[§]https://www.skybrary.aero/index.php/Safety_Culture

[¶]https://www.airbus.com/newsroom/press-releases/en/2007/11/a380-confirmed-quietest-long-range-aircraft-in-the-skies.html

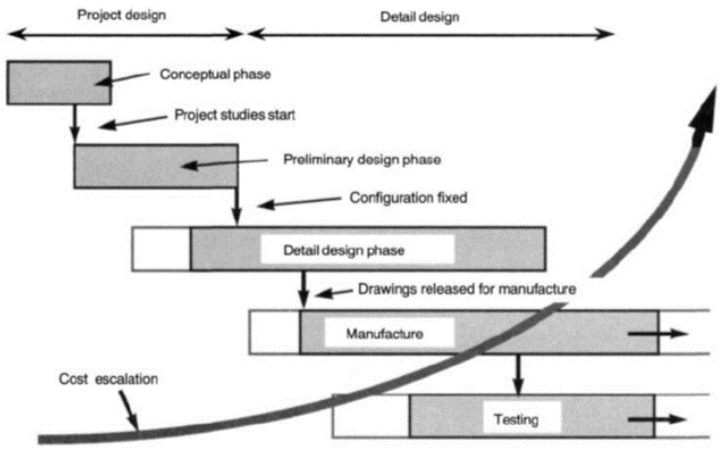

Fig. 2 Visualisatie van de gemaakte investeringen tijden het ontwerpproces van een vliegtuig [5].

2. Conceptueel Ontwerp

Nadat de ontwerp voorwaarden zijn opgesteld kan er begonnen worden met een conceptueel ontwerp. In deze fase worden alle mogelijke oplossingen bekeken. Zo heeft de TU Delft in samenwerking met KLM een Flying-V vliegtuig ontworpen dat 20% zuiniger zou zijn dan een vergelijkbaar conventioneel ontwerp. Een voorlopig ontwerp is te zien in figuur 3. In theorie biedt dit vele economische voordelen en draagt het bij aan de duurzaamheid van de luchtvaartindustrie. Hier komt dan wel een ontwerprisico bij kijken aangezien de techniek nog nieuw is en niet voldoende getest. De beschikbaarheid van nieuwe ontwerpen en technieken wordt daarom ook onderzocht en beoordeeld volgens de Technology Readiness Levels (TRL) ontworpen door NASA in de jaren '70 [7]. In de luchtvaart- en ruimtevaartsector zijn ze specifiek nuttig aangezien het ontwikkelen, testen en produceren van een nieuw vliegtuig tot wel 10 jaar kan duren. In die tijd boeken ook de gebruikte technieken progressie wat door TRL's aangeduid kan worden. De TRL kan dan aangeven of een techniek ook daadwerkelijk beschikbaar is tijdens de productiefase. Dit is ook te zien in figuur 1. Zo heeft de Flying-V nog een laag TRL waardoor niet verwacht wordt dat deze de komende 10 jaar gefabriceerd kan worden.

Uiteindelijk resulteert de conceptuele ontwerpfase in een conceptuele schets van het ontwerp. Hierbij wordt zo goed als mogelijk de vleugel- en staartgeometrie aangegeven. Ook de locatie van de motoren, het landingsgestel, de benzine tanks en passagiers- of vrachtruimte worden in kaart gebracht. Vanuit deze schets wordt een haalbaarheidsstudie uitgevoerd door middel van eenvoudige modellen, gebaseerd op statistische historische waarden [6]. Hieruit kan geconcludeerd worden of de voorwaarden vastgesteld tijdens de probleem omschrijving gehaald kunnen worden met dit concept. Wanneer dit niet het geval is kunnen de voorwaarden misschien nog aangepast worden in overleg met de klant. Vervolgens kan door middel van optimalisatie technieken gekeken worden wat dan eventueel het aantrekkelijkste vliegtuig is afhankelijk van de wens van de consument.

Dit alles leidt ertoe dat deze fase iteratief verloopt. Aan de hand van de voorwaarden wordt een concept gepresenteerd, dit leidt tot een analyse en uiteindelijk een initieel ontwerp (dit kunnen ook verschillende ontwerpen zijn). Vervolgens wordt er geïtereerd om de ideale oplossing te vinden voor het probleem. Uiteindelijk worden de verschillende ontwerpen vergeleken en worden er 1 of 2 gekozen om verder te ontwikkelen. Naast het vliegtuigontwerp wordt ook een conceptuele versie van de operationele procedures gecreëerd, dit beschrijft onder andere hoe het vliegtuig gebruikt moet worden, hoe het onderhouden moeten worden etc. Dit leidt tot een schatting van bijvoorbeeld de turnaround time (de tijd die het kost om te landen, passiers/vracht uit en weer in te laden en weer op te stijgen) en de beschikbaarheid van het vliegtuig. Ook deze eigenschappen zijn van belang voor de klant [8].

In de luchtvaart is er ook een sterk ontwikkelde veiligheidscultuur aanwezig [4]. Dit is gedeeltelijk te danken aan het intensieve certificeringsproces waar een vliegtuig doorheen gaat. Tijdens deze fase wordt de European Union Aviation Safety Agency (EASA) en de Federal Aviation Administration (FAA) al betrokken om te zorgen dat de certificatie in orde komt[‖] [9]. Zodra er een concept is, wordt dit aan de instanties gepresenteerd, die dan op hun beurt een team oprichten die de regels vaststelt die op dit ontwerp van toepassing gaan zijn. Tot slot is het sinds 2013 ook verplicht door

[‖]https://www.easa.europa.eu/easa-and-you/aircraft-products/aircraft-certification

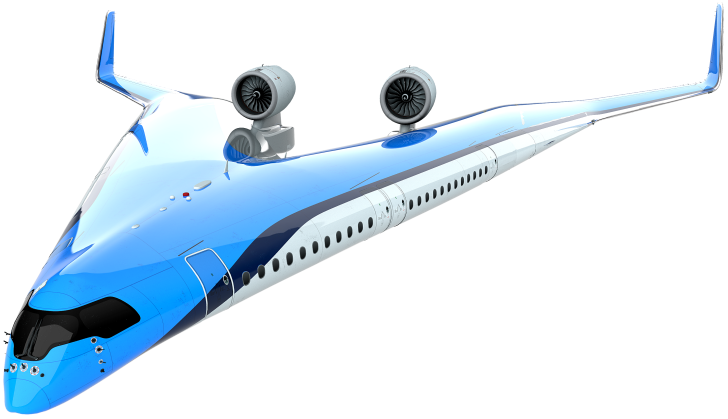

Fig. 3 Voorlopig ontwerp van de Flying-V, een samenwerking van de TU Delft en KLM[1].

[1] https://www.tudelft.nl/en/ae/flying-v/

de International Civil Aviation Organization (ICAO) om al tijdens het ontwerp van een vliegtuig een Safety Management System (SMS) te gebruiken om risico's te analyseren en alvast oplossingen aan te dragen**

3. Voorlopig Ontwerp

In de conceptuele ontwerpfase zijn alle mogelijke oplossingen bekeken en blijven alleen die ontwerpen over die haalbaar en winstgevend zijn. De grote vraagstukken zoals de vleugelconfiguratie en het type motor zijn al beantwoord. In deze fase wordt het ontwerp geanalyseerd en gesimuleerd door de desbetreffende disciplines. De komst van computerprogramma's op dit gebied heeft de kosten en doorlooptijd van het totale ontwerpproces al verbeterd [10–12]. Zo kunnen bijvoorbeeld veranderingen op aerodynamisch gebied meteen worden toegepast en de gevolgen op structureel gebied bekeken worden door de specialisten. Zogenoemde Multi Disciplinaire, Optimalisatie methodes (MDO's) combineren alle relevante disciplines in een gezamenlijk probleem wat ertoe leidt dat interacties tussen de disciplines mee worden genomen in het optimalisatie proces. Dit gebeurt niet wanneer er sequentieel naar een oplossing wordt gezocht. Daarnaast kan in deze programma's ook worden gekeken of het ontwerp geometrisch wel mogelijk is, ook wel "lofting" genoemd, en de verschillende onderdelen goed op elkaar passen. Bijvoorbeeld, zit de deur niet te dicht op de staart, past de motor wel onder de vleugel etc. Uiteindelijk levert deze fase een volledig ontwerpvoorstel op waarbij alle afmetingen vast staan, het ontwerp is dan ook "bevroren" en zal niet meer veranderen. Parallel hieraan worden ook de kosten geanalyseerd. Vervolgens wordt de GO/NO GO beslissing gemaakt. Ook nu worden de instanties nauw betrokken en worden, waar gevraagd, demonstraties gegeven van componenten en/of modellen. Tot een zekere hoogte kan dit de innovatie hinderen, soms bestaat er nog geen test voor een innovatief ontwerp en kan het niet geclassificeerd worden. Als gevolg kan deze techniek niet worden toegepast totdat nieuwe certificeringsmethode worden ontwikkeld. Dit is een interessant dilemma wat wellicht kan worden opgelost door het gebruik van gamification, de bestaande uitgebreide computerprogramma's kunnen dan worden gebruikt in gamification om bottlenecks te identificeren [13]. Dit speelt vooral een rol bij grote passagiersvliegtuigen. Kleine drones aan de andere kant zijn (nog) niet onderhevig aan de strenge testen en eisen tijdens de ontwerpfase, hierbij kunnen nieuwe technieken vrij toegepast worden. Tijdens de operationele fase gelden ook steeds strengere regels voor drones.

4. Detail Ontwerp

Als de GO beslissing genomen is, begint de gedetailleerde ontwerpfase. Hierin wordt elk sub-element van vleugellangsliggers tot elektrische componenten apart ontworpen en geanalyseerd. Ook word elk onderdeel uitvoerig getest [5]. Het vliegtuig, zoals ontworpen, wordt op ware grote in elkaar gezet om ook het totale ontwerp te kunnen testen [14]. Ook worden testvluchten gemaakt op simulatoren door testpiloten om de besturing te testen [15]. Daarnaast wordt ook het productieproces ontworpen, elk onderdeel wordt geassembleerd tot elementen en uiteindelijk tot het volledige vliegtuig. Productieontwerpers willen daarbij het ontwerp ook aanpassen om de productie goedkoper en makkelijker

**https://www.easa.europa.eu/sites/default/files/dfu/ICAO-annex-19.pdf,https://www.skybrary.aero/index.php/Safety_Culture

te maken, waarbij soms een compromis moet worden gesloten tussen productiegemak en prestatie [6]. Hierbij moet de prestatie altijd blijven voldoen aan de voorwaarde zoals omschreven in het ontwerpvoorstel. Materiaalkeuzes en assemblagetechnieken spelen een belangrijke rol voor de impact op de veiligheid van de monteurs in de korte termijn en op het milieu in de lange termijn. Daarom heeft deze fase een enorme impact op het circulaire leven van het vliegtuig. Op het moment is de norm om te kiezen voor materialen waarvan verwacht wordt dat deze over 30 jaar gemakkelijk te recyclen zijn[††], aangezien dit de levensverwachting van een vliegtuig is. Daarnaast zijn ook de verbindingsmethoden cruciaal om te zorgen dat het vliegtuig weer gemakkelijk uit elkaar kan worden gehaald, iets dat gelast is gaat moeilijker uit elkaar dan iets dat aan elkaar geschroefd zit. De gekozen materialen en methodes moeten natuurlijk wel voldoen aan de gestelde eisen tijdens de eerdere fase.

5. Productie

Als de testen succesvol zijn doorlopen en ook het productieproces ontworpen is kan het vliegtuig geproduceerd en geleverd worden. Aangezien er in de gedetailleerde designfase al is nagedacht over het productieproces kan dit veilig en gecontroleerd gebeuren. Vanaf dit moment worden investeringen op het gebied van veiligheid en gemaakte risicoanalyses dan ook terugverdiend aangezien dit het productieproces efficiënter en zonder ongelukken laat verlopen. Een goede samenwerking tussen productie-ingenieurs en vliegtuigontwerpers is nodig zodat het vliegtuig binnen de gestelde tijd gebouwd kan worden. Een geleverd vliegtuig verdient immers pas investeringskosten terug. Om op lange termijn zoveel mogelijk vliegtuigen te produceren wordt er zorgvuldig gekeken hoeveel vliegtuigen er op jaarbasis gemaakt gaan worden. Kunnen dit er meer zijn dan er worden verkocht, dan staat de productielijn een groot gedeelte van de tijd stil en kost geld. Zijn het er te weinig dan zijn de leveringstijden te lang en kopen klanten liever bij de concurrent. Het eerste vliegtuig dat van de band rolt word gebruikt om de laatste certificatietesten te doorlopen en de verplichte testvluchten te maken [9]. Mocht tijdens deze testen blijken dat bepaalde onderdelen verandert moeten worden dan moet dit gebeuren alvorens het vliegtuig gecertificeerd wordt en commercieel mag vliegen.

6. Operationele Fase

De jaren van onderzoek, simulaties en experimenten dragen allemaal bij aan de veiligheid en verdere eigenschappen (brandstofgebruik, geluidsuitstoot, etc.) van het vliegtuig tijdens de operationele fase. Deze fase bestaat uit daadwerkelijke vlieguren, het boarden van passagiers of laden/lossen van vracht en onderhoud. Mocht er tijdens deze fase iets (bijna) misgaan dan is er een plicht om dit te melden aan de instanties. Zo wordt kennis met betrekking tot veiligheid internationaal gedeeld en dit biedt voordelen voor de huidige vliegtuigen, maar ook voor toekomstige modellen.

Dat deze meldplicht werkt is voor een groot deel te danken aan het feit dat de luchtvaart probeert te leren zonder schuld toe te wijzen [4, 16]. Dit is gedeeltelijk ontstaan vlak na de Tweede Wereldoorlog door de noodzaak om het publiek te kunnen laten zien dat vliegen veilig was. Ook heeft het internationale karakter van de luchtvaart bijgedragen aan deze ontwikkeling. Dit alles heeft geleid tot een sterk ontwikkelde veiligheidscultuur in de luchtvaart.

Bij een groot incident worden nu dan ook twee onderzoeken parallel aan elkaar uitgevoerd. De rechtsgang vraagt een gerechtelijk onderzoek dat zoekt naar verantwoordelijkheid en aansprakelijkheid. Daarnaast is er een onafhankelijk technisch onderzoek dat de precieze oorzaak van het ongeluk probeert te achterhalen zonder schuld toe te kennen. Dit technische onderzoek heeft tot grote vooruitgang met betrekking tot veiligheid in de luchtvaartsector geleid. Zo zijn onderhoudsprocedures aangepast, tekortkomingen van systemen vastgesteld en is er enorme kennis toegevoegd op vakspecifieke gebieden. Deze kennis heeft ook zijn weg gevonden naar het ontwerpproces waar nu bijvoorbeeld technieken als "fail-safe", "safe life", "situational awareness" en "graceful degredation" gebruikt worden om toekomstige incidenten te voorkomen.

Het succes van onafhankelijk onderzoek zonder schuld toe te kennen heeft ook zijn weg gevonden naar het treinverkeer. In 1956 werd in Nederland het SOR opgericht, welke op een soortgelijke manier te werk gaat, later is dit ook opgezet in andere landen. Met de komst van Hogesnelheidslijnen heeft het treinverkeer ook een internationaal karakter gekregen wat op zijn beurt weer leidde tot internationale afspraken en standaarden met betrekking tot veiligheid. In de maritieme sector wordt deze manier van onderzoeken weinig toegepast. Pogingen naar onafhankelijk onderzoek behalen ook weinig succes. Hier wordt op het moment vaak de focus gelegd op de aansprakelijkheid van het ongeluk waardoor veel onderzoeken geleid worden naar menselijke fouten. Ook in het verkeer komt onafhankelijk onderzoek nauwelijks voor, dit komt ook gedeeltelijk door het hoge aantal van incidenten. Hier worden onderzoeken geleid door de politie of verzekering. Het verbeteren van de veiligheid van auto's wordt overgelaten aan de autofabrikanten zelf. Een

[††] `https://afraassociation.org/`

recent voorbeeld van een onafhankelijk onderzoek in het verkeer is het door TNO en ILT uitgevoerde onderzoek naar de Stint[‡‡].

7. Circulaire Oplossing

Op het gebied van circulaire oplossingen heeft de luchtvaart nog werk te verrichten. Op dit moment staan zogenoemde vliegtuigbegraafplaatsen vol met honderden grote en kleine vliegtuigen welke buiten werking zijn. Om dit verbeteren is in 2006 de Aicraft Fleet Recycling Association[§§] (AFRA) opgericht met als doel om de circulariteit van onderdelen en vliegtuigen te verbeteren door onderzoek en voorlichting. Hierbij is onder andere een accreditatie ontwikkeld die bedrijven kunnen ontvangen wanneer de door AFRA beschreven "best management practices" en milieu bewustheid de kern van de bedrijfsprocessen zijn. Aircraft End-of-Life Solutions[¶¶] (AELS) is een Nederlands bedrijf dat deze accreditatie heeft ontvangen. Dit bedrijf koopt oude vliegtuigen, demonteert ze, en verkoopt vervolgens de onderdelen. Aangezien onderdelen van vliegtuigen uit productie vaak ook niet meer gemaakt worden is er veel vraag naar deze onderdelen. AELS heeft sinds 2006 al meer dan 50 vliegtuigen compleet gerecycled.

Ook wordt er tijdens het ontwerp steeds meer rekening gehouden met de totale levensloop. Materiaalkeuze en assemblagetechnieken worden gekozen met recyclen in het achterhoofd waar mogelijk. Aangezien het vliegtuig waarschijnlijk pas over 30 jaar daadwerkelijk gerecycled wordt is het Technology Readiness Level van de recycle methodes vaak nog laag. Deze ontwikkelingen hebben recentelijk geleid tot de Bombardier CSeries, welke in 2016 voor zijn eerste vlucht maakte. Dit is het eerste vliegtuig dat de Environmental Product Declaration (EPD) heeft ontvangen om de impact op het milieu in zijn totale levensloop te beschrijven[***]. Daarnaast spenderen AIRBUS, Boeing en EASA jaarlijks miljoenen aan onderzoek naar het recyclen van materialen en dan specifiek koolstofvezels. Alhoewel de totale levensloop nu mee wordt genomen in het ontwerpproces wordt de komende jaren verwacht dat er meer dan 1000 vliegtuigen per jaar uit dienst zullen worden genomen. Het is dan ook van het grootste belang om hier ook nu oplossingen voor aan te dragen.

B. Boeing 737-8 Max

Recentelijk zijn twee nieuwe vliegtuigen van het type Boeing 737 MAX-8 neergestort. Hoe kon dit gebeuren in een sector die alom wordt gezien als een sector met een hoge operationele veiligheid? Al snel bleek de fout te liggen in het Manouvering Characteristics Augmentation System (MCAS) in combinatie met een kapotte invalshoek-sensor[†††] [16]. Dit leidde tot een wereldwijd verbod op het gebruik van de Boeing 737 MAX-8 en honderden vliegtuigen staan aan de grond.

De Boeing 737 Max-8 werd ontworpen als directe concurrent voor de Airbus A320 NEO. De A320 NEO werd veel verkocht vanwege zijn nieuwe motoren, welke 16% minder brandstof gebruiken, en het gebruik van Sharklets, welke de luchtweerstand verminderen door de luchtstroom over de vleugel te optimaliseren. Dit bood economische voordelen tijdens gebruik. Het succes van Airbus zorgde dat binnen Boeing een sterke drang aanwezig was om een soortgelijk vliegtuig te verkopen en leveren. Elke dag uitstel zorgde voor een significant verlies van marktpositie. Als antwoord werd een aangepaste versie van de Boeing 737 ontworpen, met aerodynamische aanpassingen en zuinigere motoren, de 737-8 MAX. Tijdens de eerste simulatortesten bleek er op vliegtuig controle gebied iets niet te deugen, een specifieke extreme manoeuvre leidde tot een pitch-up moment, veroorzaakt door een aerodynamisch effect van de nieuwe motoren, wat ervoor zorgde dat de stuurkolom niet soepel en geleidelijk bewoog zoals nodig was voor certificatie. In eerste instantie werd geëxperimenteerd met een fysieke aerodynamische oplossing. Echter bood dit niet een volledige oplossing. Uiteindelijk werd besloten het probleem softwarematig op te lossen, resulterend in het Manouvering Characteristics Augmentation System (MCAS). Wanneer het probleem zich voordeed draaide MCAS het hoogteroer omhoog wat resulteerde in een pitch-down moment. Als een gevolg bewoog de stuurkolom zich dan naar behoren. Het systeem werd geactiveerd als twee aparte sensoren deze manoeuvre herkenden, een te hoge invalshoek en een te hoge g-kracht. Ook had MCAS weinig autoriteit (zeggenschap over de besturing) aangezien het systeem alleen maar geactiveerd kon worden als zich een specifieke toestand voordeed en het hoogteroer door middel van MCAS maar 0.6 graden af kon wijken. Een interne risicoanalyse leverde op dat fouten in het systeem of de sensors weinig voorkwamen. De impact van

[‡‡] https://www.ilent.nl/onderwerpen/onderzoek-stint

[§§] https://afraassociation.org/

[¶¶] https://aels.nl/

[***] https://airlines.iata.org/analysis/end-of-life-revelations

[†††] https://www.seattletimes.com/seattle-news/times-watchdog/the-inside-story-of-mcas-how-boeings-737-max-system-gained-power-and-lost-safeguards/

een storing in het systeem werd daarnaast omschreven als "groot", een incident zou geen verwondingen veroorzaken alleen de werkdruk van de piloten verhogen. Dit maakte dat, strokend met de veiligheidseisen omschreven door de FAA, er maar 1 sensor nodig was om het systeem te opereren. Het werd als onnodig gezien om backup sensoren te plaatsen, door de invalshoek en de g-kracht te gebruiken werd er immers al een extra sensor gebruikt. MCAS werd gepresenteerd aan de certificeringsautoriteiten, de FAA en overzeese varianten, en werd niet opgemerkt als controversieel.

In 2016 na ongeveer een derde van de vliegtesten gedaan te hebben bracht Boeing veranderingen aan in MCAS. Testpiloten hadden ook dezelfde stuurkolom problemen ondervonden bij het vliegen op bepaalde lage snelheden. Om dit op te lossen werd besloten om de autoriteit en de activatie van MCAS uit te breiden. Op lage snelheden is er een grotere hoek nodig bij de staart vleugel om het zelfde effect te bereiken, MCAS mocht daarom het hoogteroer nu 2.5 graden aanpassen. Daarnaast zijn de g-krachten ook laag bij lage snelheden waardoor besloten werd om MCAS alleen nog maar door de invalshoek sensor te laten activeren, volgens de uitgevoerde risicoanalyse kon dit ook. Een nieuwe veiligheids- en risico-analyse was niet nodig, volgens Boeing en de FAA, aangezien het systeem niet in werking trad tijdens een normale vlucht. Vliegtesten waarbij een kapotte invalshoek sensor werd gesimuleerd zijn nooit uitgevoerd. In de genoemde risicoanalyses werd er volgens de richtlijnen van de FAA vanuit gegaan dat bij een fout in MCAS de piloten binnen drie seconden de fout konden herkennen en het systeem konden uitschakelen. In de praktijk bleek dat dit niet mogelijk was. Ten eerste zorgde de invalshoek sensor fout voor vele waarschuwingen waardoor de piloten afgeleid en verward werden. Daarnaast werd, vanwege de verwachte lage risico's en impact, MCAS niet genoemd in de training die piloten behoorden te volgen om de Boeing 737-8 MAX te mogen vliegen.

Dit leidde tot een systeem dat gebaseerd op 1 sensorwaarde in werking kon treden en het vliegtuig richting de grond kon duwen zonder dat dat de piloten de kennis hadden om in te ingrijpen. Uit het officiële onderzoek kunnen veel lessen getrokken worden. Hieronder worden de belangrijkste conclusies gepresenteerd met als doel om hiervan te leren zonder schuld toe te wijzen [16]:

1) MCAS was afhankelijk van 1 sensor, dit strookt niet met de fail-safe methode.
2) De training voor piloten was onvoldoende. Ze hadden niet de benodigde kennis om in te grijpen.
3) Verkeerde aannames tijdens het ontwerpproces hebben geleid tot een te kortzichtige risico analyse.
4) Het vliegtuigonderhoud was onvoldoende, er waren al eerder problemen met de sensor geconstateerd.

III. Intelligente Besturingssystemen in de Luchtvaart

Transportsystemen worden steeds zelfstandiger en intelligenter. Dit zien we in de vorm van zelf-rijdende auto's en treinen, en autonome vliegtuigen. Deze ontwikkeling roept vragen op met betrekking tot de veiligheid van deze systemen, ook denkend aan de conclusies van het onderzoek naar de incidenten omtrent de Boeing 737-8 MAX. Een Safe-by-Design strategie helpt met het in kaart brengen en verkleinen van de risico's en draagt bij aan een veilige oplossing op lange termijn.

Een veelbelovende en reeds toegepaste zelf-lerende regelaar[‡‡‡] methode is reinforcement Learning, hierbij wordt door middel van feedback signalen de "control policy" (het beleid dat de acties kiest) constant aangepast op zoek naar de optimale regelaar. Ook wanneer het vliegtuig schade ondervindt kan de zelf-lerende regelaar het vliegtuig onder controle houden aangezien deze informatie ook de regelaar bereikt, iets wat met de huidige technieken niet direct mogelijk is. Bij deze methode zijn er echter geen garanties wat betreft veiligheid aangezien de regelaar leert door middel van feedback op de gemaakte beslissingen. Ook kan de zelf-lerende regelaar de control policy aanpassen naar een onveilige regelaar. De optimale control policy vinden kan lang duren omdat in theorie alle toestand-actie combinaties geprobeerd moeten worden. Bij een vliegtuig met meerdere toestanden en meerdere acties welke vaak nauwkeurig gediscretizeerd worden zijn dit bijna oneindig veel combinaties. Dit leidt tot het zogenaamde "exploration-exploitation" (leren-benutten) dilemma [17, 18]. Wanneer het systeem niet genoeg tijd krijgt om te leren wordt de optimale regelaar nooit gevonden. Wordt er echter te veel tijd besteed aan het leren dan duurt het lang voordat de opgedane kennis benut wordt. Daarnaast speelt ook veiligheid een rol. Tijdens het leren leidt niet elke actie tot een veilige toestand, wat het leren van de complete toestand-ruimte gevaarlijk maakt. Tijdens computersimulaties is dit geen groot probleem, in het ergste geval moet de simulatie opnieuw uitgevoerd worden. Echter bij de toepassing op een vliegtuig kan dit betekenen dat het vliegtuig in de leerfase in een overtreksituatie terecht komt omdat de invalshoek te groot wordt, of een gevaarlijke duik maakt met alle gevolgen van dien. Dit probleem is niet specifiek voor de luchtvaart maar komt voor in alle sectoren waar veiligheid een rol speelt. Om dit te verbeteren moet er onderzoek gedaan worden naar methodes om deze veiligheidsgaranties toe te voegen. Ofwel hoe kan het systeem de control policy optimaliseren zonder onveilige acties te nemen. In dit onderzoek

[‡‡‡]Een regelaar van een dynamisch systeem controleert de toestand van het systeem door te kijken naar de fout tussen de gewenste en de gemeten toestand.

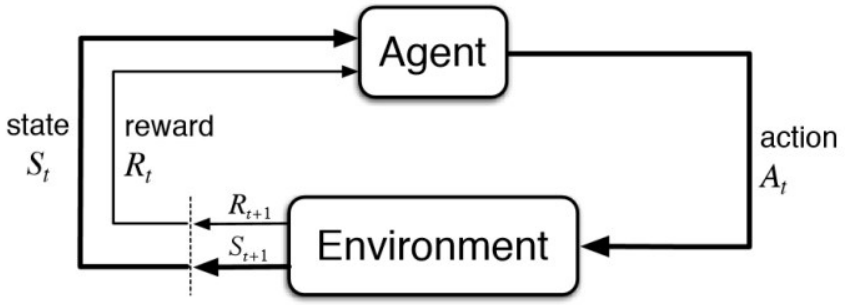

Fig. 4 Basisprincipe achter reinforcement learning. Een reinforcement learning agent maakt een beslissing a. Aan de hand hiervan bepaalt de omgeving de nieuwe toestand s en de beloning r [19].

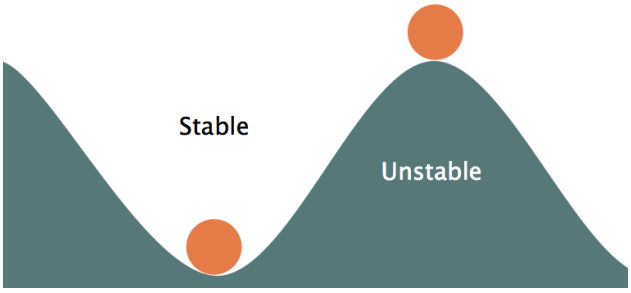

Fig. 5 De linker bal komt overeen met een stabiel vliegtuig, de bal zal bij een kleine tik terugkeren naar de initiële positie. De rechter bal is onstabiel, een kleine tik heeft nu grote gevolgen.[3]

[3] Image from `http://software.imdea.org/projects/averist/Figures/stab_ball.png`

wordt hier aan bij gedragen door eerst te bekijken hoe veiligheid gedefinieerd is in flight control (vliegtuig controle systemen), vervolgens zal safe reinforcement learning uitgelicht worden.

A. Veiligheid in Vliegtuig Regelaars

In deze sectie wordt in het kort uitgelegd hoe veiligheid gedefinieerd is binnen flight control. Veiligheid wordt uitgedrukt in de stabiliteit van het vliegtuig en daarnaast is er een zogenoemde "safe flight envelope" waar het vliegtuig zich ten allen tijde binnen moet bevinden. Een soortgelijke benaming bij reinforcement learning zou kunnen zijn "convergentie" en het blijven binnen de "veilige toestand". Beiden worden hieronder verder uitgelegd.

Een stabiel vliegtuig draagt bij aan de veiligheid omdat deze zelfstandig terugkeert naar de initiële positie na een verstoring zoals een windvlaag of turbulentie. Hiervoor hoeft de piloot niets te doen. Een onstabiel vliegtuig daarentegen zal de kleinste verstoring versterken en afwijken van de initiële positie. Dit is afgebeeld in figuur 5. Bij het gebruik van reinforcement learning is stabiliteit lastig uit te drukken. De regelaar verandert immers constant. Dit creëert ook moeilijkheden tijdens de certificatie van een vliegtuig [20]. De huidige methodes kunnen niet gebruikt worden om adaptieve regelaars te certificeren [21]. Er wordt al onderzoek uitgevoerd naar nieuwe certificeringsmethodes. In [22] wordt bijvoorbeeld voorgesteld dat regelaars niet langer binnen stabiliteitmarges moeten vallen, maar dat ze kunnen demonstreren een referentie te kunnen volgen waarbij ze binnen een maximum afwijking van deze referentie blijven.

De safe flight envelope van een vliegtuig laat zien in welke toestanden het vliegtuig zich mag bevinden volgens de ontwerplimieten. In tegenstelling tot de stabiliteit welke verbeterd kan worden door regelaars, staan de ontwerp-limieten vast. Bijvoorbeeld, aerodynamische limieten leiden tot een maximale invalshoek van het vliegtuig, en structurele limieten hebben een invloed op de maximale g-krachten die het vliegtuig aankan. Variabelen zoals het huidige gewicht, de hoogte, of de snelheid hebben invloed op deze limieten. Moderne vliegtuigen hebben vaak een flight envelope protection systeem waardoor het voor piloten onmogelijk wordt om het vliegtuig uit de safe flight envelope te halen [23]. Daarnaast kunnen lokale luchtvaart autoriteiten snelheid- en/of hoogte-limieten op leggen. Het identificeren van al bovengenoemde limieten is op zichzelf staand al een complex probleem.

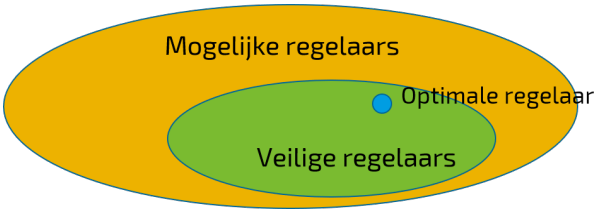

Fig. 6 Visualisatie van de taak van een zelf-lerend systeem. Het systeem zoekt naar de optimale regelaar, maar mag daarbij geen onveilige regelaars proberen.

De safe flight envelope is direct gerelateerd aan de veilige toestanden die een reinforcement learning systeem mag betreden en deze zijn vaak al van te voren bekend. Deze kennis kan bijdragen aan het veilig leren van een reinforcement learning systeem. Door dit van te voren mee te geven hoeft het systeem deze kennis niet meer te ervaren.

B. Safe Reinforcement Learning

In reinforcement learning is het systeem constant op zoek naar de optimale regelaar. Alhoewel verschillende methodes het anders aanpakken blijft de essentie hetzelfde, ook uitgebeeld in figuur 4. 1) Er wordt eerst een actie genomen, 2) waarna het effect van de actie bekeken wordt door de nieuwe toestand en de feedback te bekijken. 3) Vervolgens wordt de huidige control policy aangepast op zoek naar verbetering. 4) Dit wordt herhaald totdat de optimale regelaar gevonden is. Niet elke control policy is veilig, door aanpassingen aan de control policy kan dus ook voor onveilige acties gekozen gaan worden. In figuur 6 is te zien hoe uit alle mogelijke regelaars maar een selecte groep daadwerkelijk het vliegtuig veilig kan besturen. In die groep veilige regelaars bevindt zich ook de optimale regelaar welke voor de beste prestaties zorgt. Tijdens het vliegen kunnen deze regio's ook veranderen. Wanneer bijvoorbeeld de snelheid significant wordt verhoogd is er een andere regelaar nodig om het vliegtuig veilig te besturen.

Om veiligheidsgaranties toe te voegen aan reinforcement learning moet men realiseren waarom de leerfase nodig is. Zonder de leerfase zou het systeem geen kennis kunnen opdoen en de huidige regelaar niet kunnen verbeteren. In de praktijk krijgen foute beslissingen vaak een grote virtuele straf waardoor het systeem deze actie in de toekomst probeert te vermijden. Het ontdekken is nodig om kennis op te doen. Door het systeem van te voren al bekende kennis mee te geven hoeft het deze kennis niet te leren door middel van fouten en kan het systeem in theorie zichzelf verbeteren zonder onveilige acties te proberen.

Deze kennis meegeven aan het reinforcement learning systeem kan op verschillende manieren. Hieronder worden twee methodes beschreven die ook toegepast zijn in de luchtvaart waarbij state-of-the-art toepassingen worden beschreven. Ten eerste wordt "constrained exploration" (begrensde ontdekking) uitgelegd. Wanneer constrained exploration wordt toegepast krijgt het systeem alle vrijheid om te ontdekken, maar van te voren worden limieten gegeven die het systeem niet mag overschrijden. Bij toepassing in de luchtvaart zouden deze limieten bijvoorbeeld de safe flight envelope kunnen zijn zoals beschreven in sectie III.A. Volgens [17] is deze methode uitermate geschikt in omgevingen waar fouten een hoog risico met zich mee brengen. Met deze methode wordt externe kennis overgedragen in de vorm van limieten. Daarnaast heeft het systeem ook een nauwkeurig model van de omgeving nodig om te kunnen voorspellen of de limieten daadwerkelijk overschreden worden bij het toepassen van de actie. Dit model moet dan ook van te voren bekend (of voortijdig geïdentificeerd) zijn om de methode succesvol toe te passen. Een voorbeeld hiervan is te vinden in [24]. Hier wordt gedemonstreerd hoe een gesimuleerd ruimteschip zich van A naar B leert te bewegen zonder buiten een denkbeeldige gang te dwalen. De onderzoekers laten het reinforcement learning systeem ontdekken, maar controleren vervolgens elke actie met een voortijdig geleerd lineair model. Mocht de actie volgens dit model leiden naar een onveilige toestand, i.e. buiten de denkbeeldige gang, dan wordt de actie vervangen door de dichtstbijzijnde actie die het schip veilig houdt. Deze actie wordt ook gevonden met behulp van het lineaire model. Dit leidt ertoe dat het ruimteschip zichzelf leert besturen zonder ooit een onveilige toestand mee te maken.

Ten tweede wordt de risico-sensitieve criteria beschreven. Bij deze methode wordt naast de toestand en het feedback signaal zoals afgebeeld in figuur 4 ook aangenomen dat het risico van de huidige toestand kan worden ingeschat. Dit risicosignaal kan dan gegenereerd worden door extra sensoren of er kan worden gekozen om van te voren limieten op te geven. Wanneer het systeem dan dichter bij de limiet komt, zal het risico van de toestand groter worden. Door vervolgens te optimaliseren voor een hoge beloning met een laag risico, wordt veilig ontdekken aangemoedigd. Extra kennis wordt nu overgedragen aan het systeem aan de hand van vastgestelde limieten en/of extra sensoren, in tegenstelling tot bij

constrained exploration is nu geen model van de omgeving nodig. In [18] wordt een vorm van risico-sensitieve criteria toegepast. Dit wordt gecombineerd met een back-up route naar een veilige toestand, deze route wordt geleerd aan de hand van historische waarden. Een drone krijgt de taak om een virtuele kamer in kaart te brengen zonder de muren, het plafond, of de grond te raken. Van te voren weet de drone niet waar deze objecten zich bevinden. Wanneer de drone zich binnen een meter van de muur of een halve meter van het plafond of de grond bevindt krijgt deze een waarschuwing. Dan wordt een back-up route geactiveerd naar een veilige positie om vanuit daar opnieuw te beginnen. Demonstraties laten zien dat de drone de muur niet raakt zelfs als het reinforcement learning systeem zonder de veiligheidsmaatregelen compleet willekeurige acties maakt.

IV. Conclusie

Het doel van dit onderzoek is tweeledig, ten eerste om een analyse te maken van de totale levensloop van een vliegtuigontwerp om inzicht te geven in hoe er wordt omgegaan met veiligheid in een multidisciplinair project. Specifiek in de luchtvaart is er een sterk ontwikkelde veiligheidscultuur aanwezig welke ook wordt aangemoedigd door Safe-by-Design. Deze is noodzakelijk om het publiek vertrouwen te geven in de luchtvaart. Ook biedt deze veiligheidscultuur financiële voordelen. Wanneer er een nieuw model vliegtuig ontworpen wordt zet een bedrijf vaak zijn toekomst op het spel. Dit vanwege de grote investeringen welke na 7 tot 10 jaar pas worden terugverdiend. Het lange termijn safe-by-design denken zorgt dan dat er geen onnodige risico's worden gelopen en dat de investering zonder onverwachte kostenposten kan worden terugverdiend. Daarnaast worden Technology Readiness Levels gebruikt om de vooruitgang van techniek aan te duiden. Ook ondergaan nieuwe ontwerpen in de ontwerpfase al uitgebreide certificeringen om de veiligheid van het uiteindelijke ontwerp te waarborgen. Dit certificeringsproces volgt de ontwikkeling van het vliegtuig op de voet. Alhoewel de uitgebreide certificeringen bijdragen aan de veiligheid hindert dit de innovatie, huidige certificeringsmethodes zijn niet altijd in staat om innovatieve oplossingen te certificeren. Om de samenwerking tussen de verschillende disciplines te verbeteren wordt gebruik gemaakt van Multi-Disciplinaire Optimalisatiemethodes (MDO) op basis van computermodellen en simulaties. Hierdoor worden ontwikkelingen gemakkelijk gedeeld en zijn interacties tussen disciplines al vroeg mogelijk. Ook leidt dit ertoe dat er iteratief geoptimaliseerd kan worden om sneller het optimale ontwerp te vinden. Specialisten uit andere gebieden worden ook geconsulteerd waar nodig. Zo hebben productie-ingenieurs input in het ontwerp van het vliegtuig om het productieproces te vergemakkelijken, ook is er op dit moment veel interesse in end-of-life oplossingen voor vliegtuigen waardoor het circulaire denken nu ook zijn weg in het ontwerpproces heeft gevonden.

Daarnaast worden incidenten in de luchtvaart onafhankelijk onderzocht zonder te zoeken naar aansprakelijkheid. Deze manier van onderzoeken heeft, naast het vinden van korte-termijn oplossingen voor incidentele ongelukken, ook nieuwe technieken en standaarden voor toekomstige ontwerpen voortgebracht. Incidenten op het spoor worden op soortgelijke manier onderzocht, maar in de maritieme sector en in het wegverkeer wordt dit tot op heden nauwelijks toegepast.

Om intelligente systemen toe te passen in de luchtvaart is het van belang om veiligheidsgaranties te kunnen geven. Een Safe-by-Design intelligent systeem voor vliegtuigen zal zijn kennis over de veiligheid van de huidige vliegtuigtoestand op meerdere manieren moeten vergaren om zo effectief tot een totaalbeeld te komen. Ook kan het helpen om vooraf kennis mee te geven over de mogelijk veilige acties. Dit vereist meer onderzoek alvorens het in de praktijk toegepast kan worden.

Daarnaast is het interessant om te kijken of Safe-by-Design Gamification ook in de luchtvaart kan leiden tot een versnelling van innovatie. Gamification, in combinatie met de huidige MDO-tools en kennis op het gebied van veiligheid, kan snel tot nieuwe ideeën leiden.

References

[1] Bojarski, M., Del Testa, D., Dworakowski, D., Firner, B., Flepp, B., Goyal, P., Jackel, L. D., Monfort, M., Muller, U., Zhang, J., et al., "End to end learning for self-driving cars," *arXiv preprint arXiv:1604.07316*, 2016.

[2] Ng, A. Y., Coates, A., Diel, M., Ganapathi, V., Schulte, J., Tse, B., Berger, E., and Liang, E., "Autonomous inverted helicopter flight via reinforcement learning," *Experimental robotics IX*, Springer, 2006, pp. 363–372.

[3] Zhou, Y., Van Kampen, E., and Chu, Q. P., "Incremental approximate dynamic programming for nonlinear flight control design," *Proceedings of the 3rd CEAS EuroGNC: Specialist Conference on Guidance, Navigation and Control, Toulouse, France, 13-15 April 2015*, 2015.

[4] Stoop, J. A., and Kahan, J. P., "Flying is the safest way to travel: How aviation was a pioneer in independent accident investigation," *European journal of transport and infrastructure research EJTIR, 5 (2)*, 2005.

[5] Jenkinson, L., Simpkin, P., and Rhodes, D., *Civil jet aircraft design*, American Institute of Aeronautics and Astronautics, Inc., 1999.

[6] Raymer, D., *Aircraft design: a conceptual approach*, American Institute of Aeronautics and Astronautics, Inc., 2018.

[7] Mankins, J. C., "Technology readiness levels," *White Paper, April*, Vol. 6, 1995, p. 1995.

[8] Bazargan, M., "A linear programming approach for aircraft boarding strategy," *European Journal of Operational Research*, Vol. 183, No. 1, 2007, pp. 394–411.

[9] De Florio, F., *Airworthiness: An introduction to aircraft certification and operations*, Butterworth-Heinemann, 2016.

[10] Rocca, G. L., and L. Van Tooren, M. J., "Knowledge-based engineering approach to support aircraft multidisciplinary design and optimization," *Journal of aircraft*, Vol. 46, No. 6, 2009, pp. 1875–1885.

[11] Nagel, B., Böhnke, D., Gollnick, V., Schmollgruber, P., Rizzi, A., La Rocca, G., and Alonso, J. J., "Communication in aircraft design: Can we establish a common language," *28th International Congress of the Aeronautical Sciences*, 2012, pp. 1–13.

[12] Ciampa, P. D., and Nagel, B., "The AGILE Paradigm: the next generation of collaborative MDO," *18th AIAA/ISSMO multidisciplinary analysis and optimization conference*, 2017, p. 4137.

[13] Roelofsma, P., "Gamification for Safe by Design of Human - Avatar and Robot Care Systems," 2019.

[14] Li, Z., Xi, Y., Shi, Y., Wang, S., and Wang, X., "Modular design of iron bird for modern aircraft," *2016 IEEE International Conference on Aircraft Utility Systems*, 2016, pp. 1133–1137.

[15] Kroll, N., Abu-Zurayk, M., Dimitrov, D., Franz, T., Führer, T., Gerhold, T., Görtz, S., Heinrich, R., Ilic, C., Jepsen, J., Jägersküpper, J., Kruse, M., Krumbein, A., Langer, S., Liu, D., Liepelt, R., Reimer, L., Ritter, M., Schwöppe, A., Scherer, J., Spiering, F., Thormann, R., Togiti, V., Vollmer, D., and Wendisch, J.-H., "DLR project Digital-X: towards virtual aircraft design and flight testing based on high-fidelity methods," *CEAS Aeronautical Journal*, Vol. 7, No. 1, 2016, pp. 3–27.

[16] KNKT, "Aircraft Accident Investigation Report PT. Lion Mentari Airlines Boeing 737-8 (MAX)," , 2019. URL "http://knkt.dephub.go.id/".

[17] Garcia, J., and Fernandez, F., "A Comprehensive Survey on Safe Reinforcement Learning," *The Journal of Machine Learning Research*, Vol. 16, 2015, pp. 1437–1480.

[18] Mannucci, T., Van Kampen, E. J., De Visser, C., and Chu, Q., "Safe Exploration Algorithms for Reinforcement Learning Controllers," *IEEE Transactions on Neural Networks and Learning Systems*, Vol. 29, No. 4, 2018, pp. 1069–1081.

[19] Sutton, R. S., Barto, A. G., et al., *Introduction to reinforcement learning*, Vol. 2, MIT press Cambridge, 1998.

[20] Bhattacharyya, S., Cofer, D., Musliner, D. J., Mueller, J., and Engstrom, E., "Certification Considerations for Adaptive Systems," Tech. rep., 2015. URL http://www.sti.nasa.gov.

[21] Stepanyan, V., Krishnakumar, K., Nguyen, N., and Van Eykeren, L., "Stability and Performance Metrics for Adaptive Flight Control," *AIAA Guidance, Navigation, and Control Conference*, American Institute of Aeronautics and Astronautics, Reston, Virigina, 2009, pp. 1–19.

[22] Jacklin, S., "Closing the Certification Gaps in Adaptive Flight Control Software," 2012. URL https://ntrs.nasa.gov/search.jsp?R=20090026333.

[23] Briere, D., and Traverse, P., "AIRBUS A320/A330/A340 electrical flight controls - A family of fault-tolerant systems," *FTCS-23 The Twenty-Third International Symposium on Fault-Tolerant Computing*, 1993, pp. 616–623.

[24] Dalal, G., Dvijotham, K., Vecerik, M., Hester, T., Paduraru, C., and Tassa, Y., "Safe Exploration in Continuous Action Spaces," *arXiv preprint arXiv:1801.08757*, 2018. URL http://arxiv.org/abs/1801.08757.