State of the art of unmanned aircraft transport systems in industry related to risks, vulnerabilities and improvement of safety

S.O. Johnsen, T.E. Evjemo
SINTEF, Trondheim, Norway. E-mail: Stig.O.Johnsen@sintef.no

This paper discusses state of the art of unmanned aircraft systems (UAS), drones (unmanned aerial vehicle -UAV's) and control infrastructure. The focus has been to explore risks, vulnerabilities and safe use of UAS in industrial operations. The use of UAS has been in rapid expansion in governmental areas (monitoring, military applications) and in the public domain (leisure, photography, transportation, monitoring). Several vulnerabilities have been identified. Few empirical analyses of operations, incidents and successful recoveries are available due to limited reporting. However, safety information from military drone operations are available. The three research questions in this paper are to describe planned use of UAS, major risks and benefits of UAS, and needed research, requirements and rules to improve safety and resilience of operations. We have explored the status of research in Norway, we have performed a literature review of autonomy in aviation, and we have explored relevant cases of industrial transport systems. Our findings indicate that rules and regulations are lagging development of technology and that there is poor focus on major risks related to human factors in engineering, design and operations. To ensure that safety and resilience is in focus from design, there is a need to define scope (i.e. control system as part of UAS) establish functional guidelines (such as human factors guidelines) and improve regulatory frameworks.

Keywords: Unmanned aircraft system, Autonomous aircraft, rules, regulation, safety, security, Human Factors.

1. Introduction

In this paper we are exploring safety of unmanned aviation systems (UAS) based on drones (unmanned aerial vehicle -UAV's). Safety of UAS is influenced by the practices of aviation, such as rules, regulation, organisation, technology and human factors. Learning from existing practice is needed since aviation has ultra-high safety, Amalberti (2017), with an accident rate of 1.08 accidents per 1 million flights. The International Air Transport Association (IATA) represents 290 airlines in 120 countries and carries 82% of the world's air traffic. IATA achieves "ultra-safety" in their aviation operations, having no hull-losses in 2012 or 2017 with jet or turboprop equipment. The practices from general aviation should be helpful when establishing safety of UAS.

By *autonomy* we mean a system that can make a choice free from outside influences and change its initial way of programmed actions (having some notion of "free will", where actions are not determined completely by previously existing causes, i.e. non-deterministic Hoefer, 2003). By *automated* we mean a system that will do exactly what it is programmed to do. This is based on the taxonomy and discussion of autonomy from Vagia et al. (2016). In Parasuman and Riley (1997) automation and autonomy is described as "*The execution by a machine agent (usually a computer) of a function that was previously carried out by a human*".

Manned flight operations have been highly automated, but full autonomous operations have not been established yet. One issue that challenges autonomy is handling of the unexpected vs the human ability to act and recover. One successful recovery that has been used to discuss the challenges of autonomy has been the incident of US Airways Flight 1549 from New York City's LaGuardia Airport on January 15, 2009, that lost all engine power by hitting a flock of Canada geese. Unable to reach any airport, the pilots glided the plane to a ditching in the Hudson River, and all 155 people aboard were rescued, NTSB (2010). An incident that could have been difficult to handle by autonomy at present. Discussing automation, we have adopted level of automation (LoA) from SAE (2016); describing LoA through responsibilities between pilot and aircraft:

Table 1. Levels of Automation – responsibilities

LoA	**Human Pilot**	**Aircraft control**
1:No automation	All operations	Warns Protect
2:Limited assist; Auto throttle	Drives In-the-loop	Guides Assist
3:Assist, Tactical; Supervised	On-the loop Pilot monitors all time	Manage movement within defined limits
4:Automated Assist Strategic	Out-of-loop Asked by system	Flies, but may give back control
5: Autonomous	Completely out-of-loop	Flies with graceful degradation

Proceedings of the 29th European Safety and Reliability Conference.
Edited by Michael Beer and Enrico Zio
Copyright ©2019 by ESREL2019 Organizers. *Published by* Research Publishing, Singapore
ISBN: 981-973-0000-00-0 :: doi: 10.3850/981-973-0000-00-0 esrel2019-paper

The actual control (responsibilities) can be performed remotely or locally (by a human or through machine control).

An UAS is an aircraft that may be controlled remotely (through LoA:1 to Loa:4) as a Remotely Piloted Aircraft System – RPAS or flying fully autonomously (as defined by LoA:5).

Safety is related to accidental harm, while security is related to intentional harm. Safety is defined as: "*the degree to which accidental harm is prevented, reduced and properly reacted to*", Firesmith (2003). Security: "*the degree to which malicious harm is prevented, reduced and properly reacted to*".

Drones have often been used in tasks being dangerous, dirty or dull. Thus, safety and security have often been the principal drivers when using UAS. Use of UAS is expanding, a compound annual growth rate of 100% has been estimated in Europe and in the US from 2016 (Quilter et al., 2017). By the end of 2017 there were approx. 1,1 million UAS in the US.

There is a need to ensure high reliability, safety and security when UAS is being used in critical operations such as transport of medical supplies (blood, medicine). As the use expands, there is a need to limit the vulnerability of UAS.

1.1 *Scope – equipment and airspace*

The UAS consist of the drone (with a network of sensors – navigation system, different electronic systems, actuators, power system, mainframe, payload) and communication links to the environment (such as a simple controller or ground control systems).

The airspace is divided into regulated/ controlled airspace and unregulated airspace. Individuals can operate UAS in unregulated airspace, however sharing controlled airspace between manned aircrafts and UAS is at present a challenge. In the US, regulation is developed through the Federal Aviation Administration (FAA), while in EU through European Aviation Safety Agency (EASA). The regulators - FAA and EASA is challenged by the rapid technological development of UAS, and lags somewhat in the development of regulation, Altawy et al. (2017).

There is a need to define the operational tasks to explore the risks of UAS. Key tasks being performed in preparation and operations of UAS are: -Flight Planning; Start & Taxi; Take-off & Departure; en-route; Aerial Work; Descent & Approach; Landing; Halt/ Post landing; and Handover activities. Aerial work can encompass delivery of supplies such as dropping goods by parachutes. During these tasks, communication is needed and is on-going between the pilot and the UAS. There may be a need to communicate to Air traffic Control; to other aircrafts; to other actors such as Police (in case of accidents).

1.2 *Challenges and research questions*

Development and implementation of UAS is dependent on many factors, such as benefits given by the technology but also challenges of safety and security. Significant benefits are achieved using UAS, such as saving lives by delivering blood or medical supplies faster (as reported in Time, 2018); by reducing risks or replacing dangerous and error prone helicopter operations. A key factor of this replacement is safety and security of UAS operations. Our perspective of safety and security is based on an integrated view of organisational issues, technology and human factors. As discussed in Lund and Aarø (2004), risk reduction must be based on a broad set of actions such as organisational issues (regulation, procedures) technical design, and human factors issues such as usability, training and awareness.

The UAS is vulnerable to attacks through the systems it consists of, such as sensors, actuators, communication links and ground control systems. As an example, an Iranian cyber warfare unit was able to land a US drone based on a spoofing attack modifying global positioning system-GPS data (Altawy et al. 2017).

In Petritoli et al. (2017) the Mean Time Between Failures (MTBF) was estimated for drones, being around 1000 hours. Approximately 100 times higher than MTBF in manned flights. Based on 1000 - failures, the division of failures were in: Power plant (411); Ground Control system (273); Navigation system (146); Electronic system (67); Mainframe (54) and Payload (53). However, the risk of these failures is dependent on the consequences of the failures such as weight (lightweight drone observation, or heavy industrial transport) and the area of use (in a urban area/ city or in remote and sparsely populated areas). Failure of power system can have significant impact in an industrial (heavy) drone flying in a city and crashing by high speed (i.e. high energy impact).

Experiences of UAS from the US government, Waraich et al. (2013), documents that mishaps may happen (i.e. 50-100 mishaps occur every 100,000 flight hours' vs human-operated aircraft where there is one mishap per 100,000 flight hours). The mishap rate of UAS is significantly higher than manned operations. Main causes are related to poor attention to human factors science, such as poor design of ground control centres, Waraich et al. (2013), Hobbes et al. (2014).

Thus, we see the need to explore the context and actual use of the UAS to discuss risks and mitigating actions such as regulation.

The three research questions in this paper are:

- What is the status of planned use and research of UAS in transport systems?
- What are the major risks and benefits of unmanned aircraft transport systems?

- What are needed mitigation in research, requirements and rules to improve safety and resilience of UAS operations?

2. Methods

To describe the planned use of UAS we have performed a review of research and innovation from the research database of the Norwegian research council in the period 2008 to 2021 and reviewed drone research. The search string used were UAS, UA* or Drones. We excluded project with grants below USD 12000 (NOK 100 000). The projects are listed by their short descriptive name found in the database.

We have performed a literature review in Web of Science and Scopus based on the search string "Safety and Security of Unmanned Aircraft Systems/ or Drones /or UAS". We limited the search to the period 2013 to 2019 to get current studies, and excluded papers not written in English.

As a part of an aviation study focusing on safety and autonomy in Norway, (Evjemo, 2018), seven interviews (of regulators, fixed wing and drone pilots, flight controllers) were performed to discuss safety of increased level of automation in manned flights and use of UAS.

3. Results and discussion

In the following we have described the use of UAS; the planned use of UAS based on research, then the result of a literature review of safety and security; and lastly key result from interviews. UASs are used in many different areas, we have listed some cases:

1) Providing Internet access in rural areas or in areas when there is a special need (He et al, 2017)
2) Cinematography and aerial photography – (Rao et al, 2016)
3) Inspection of equipment to improve quality or avoid dangerous work (Rao et al, 2016). Cases financed by Norwegian research council: Inspection of power lines by artificial intelligence (AI); inspection of storage tanks/ facilities to avoid dangerous conditions, see section 3.1
4) Ambulance and medical services, delivering medicine, aid, medical equipment fast and safe to remote areas or in a crisis; as an example, DHL is regularly delivering medicine twice a day to the island of Luist (Altawy et al, 2016) and blood supply is delivered by drones in Rwanda from 2016 within 30 minutes (Time, 2018).
5) Deploying UAS carrying specialized medical equipment in response to medical emergencies (Balasingam, 2017).
6) Disaster help – to get overview of damages, placement of people or infrastructure, deliver critical equipment or supplies fast; UAS were used in the Fukushima Nuclear disaster to deliver food supplies and in assessments of radiation levels within the reactor buildings. Chowdhury et al (2017) Balasingam, (2017).
7) Farming/ crop management (Rao et al, 2016).
8) Illicit transportation: Drug smuggling or delivering goods/ drugs to prison inmates, Altawy et al. 2016)
9) Drones used as physical weapons (both through military use and others) or as cyber weapons to spread malware (Valente, 2017)
10) Monitoring and survey of areas (i.e. monitoring of seaways), border control (Pathiyil, et al. 2017)

Barriers for rapid deployment of this technology has often been the lack of timely and risk-based legislation, (Pathiyil, et al. 2017). However, EASA have drafted legislation for UAS to fly safely in the EU (EASA 2018) – providing basic guidelines for safety, security and privacy. Including extent of how other traffic or people on the ground can be endangered, drone certification, insurance, protection of environment (in relation to noise and pollution) and security and privacy concerns.

3.1 *Planned use of UAS based on research*

In the following section we have documented research and innovation projects financed by the research council in Norway. We found 31 projects that were financed. The financing in the period from 2008 to 2021 has increased significantly, as shown in the following Table 1.

Table 1. Investments in UAS research increasing

Period - Year	Financing
2008-2012	35,9 Mill NOK
2013-2017	56,7 Mill NOK
2018-2021	119,3 Mill NOK

Thus, there is an increased focus on research related to UAS. Exploring different application areas, we list the found projects by their short name from the database (*denotes safety focus), allocated to the following areas:

- **Marine (7):** *Safe lifting between supply ships and oil platforms using drones; *Safe maritime landing for UAS; Un-manned operation of Fish Farming; *ASSUR-airborne ship safety UAS to look for man-overboard or oil spills; *Ice monitoring and technological improvements in communication; UAS in North for Ice monitoring; *In ship - autonomous inspection of storage tanks.

- **Technological improvement (7):** Improved batteries for drones; Development of composite electrical motor for Drones; Development of hybrid propulsion of UAS; Vertical take-off and landing; Scout for inspection of equipment; Mosquito – technology for small scale UAS; *DroneSafe – developing world class drones for recording in constrained areas.
- **Power line inspection (5):** Maintenance; *Fault detection (by use of AI); *Autonomous inspection; *Smart Electricity Grid Inspection; Remote Inspection of Wooden Utility Poles.
- **Air control systems (3):** Air traffic management of UAS; Autopilot design for UAS in extreme conditions; Low altitude UAS communication and tracking;
- **Biological/Farming (2):** Survey of plant parasites; Counting of seal population;
- **City management (2):** Observe building changes in a city based on Drone surveys; *Inspection of critical infrastructure – status of bridges built in concrete
- **Health Care (2):** *UAS for fast and secure transportation of blood products and biological material; Development of commercial medical transport service;
- **Geographical survey (1):** Measurement of gravity and magnetic fields.
- **Societal issues (1):** responsible adoption of visual surveillance technologies in the news media.

Of these cases we observe that 10 of 31 projects (marked by *) used improved safety in operations as a key argument for the project, however there was poor focus on security.

Living in Norway - a decentralized country with vast distances, it was surprising that the following were not funded: -disaster services; use of drones to speed up deliveries of critical supplies between remote areas; use of drones to establish efficient parcel deliveries.

There has been little focus on safety-oriented research to improve MTBF such as reliability of the power system and necessary research and requirements in relation to ground control systems. When looking at safety challenges identified from use of drones (Petritoli et al. 2017), the main challenges has been related to Power plant; Ground Control system; Navigation system; Electronic system; Mainframe and Payload. The human factors deficiencies of ground control systems as mentioned in Waraich et al. (2013) or Hobbes et al. (2014) has not been sufficiently mitigated.

Implementation of new technology are dependent on development of societal and organisational aspects (Ethics, rules, regulation, communication, accident reporting systems, stakeholder development), user needs and quality of Human Factors design in operation of new technology. However – these areas have not been mentioned in the identified research projects.

The Norwegian Government has published a strategy for the use of Drones/ UAS in Norway, ND (2018). Key strategies are: Establish rules and regulation; Focus on safety; Inform users about relevant rules and regulations; Prioritize use of drones in government; Support research and innovation related to the use of UAS. The strategy is somewhat sketchy related to ethical and social aspects; security of drones related to vulnerabilities/ mitigating actions; and documentation of known safety challenges.

In summary, based on the project having acquired research financing there seems to be a need for more systematic research and focus on:

- **Ethical and social aspects of the use of UAS – as an example the importance of building networks/ societal actor networks to support safe and secure use of Drones** (by co-opting network such as Norwegian UAS member association)
- **Human Factors based design, such as Human factors Guidelines for Ground Control centres** - to support improved quality of operations
- **Security and safety of UAS,** especially UAS to be used in an industrial setting. Need systematic gathering of operational data, more research and development to improve safety of industrial drone transportation, with focus on major risks and improvement of MTBF (based on registers of incidents).
- **Regulation to support deployment of industrial UAS** in urban areas, and autonomous transport in rural areas
- **Regulation and research to integrate UAS in controlled airspace**
- **Poor focus on development of methods to build resilience, i.e.** to assess vulnerabilities, risks and how to mitigate the unexpected through resilience – (i.e. poor focus on resilience engineering of autonomous systems).

3.2 *Literature review – safety and security*

Security threats are dependent on context, capabilities/intent of adversary and use. Scope of security must address risk of physical harm but also address confidentiality, integrity of information and availability. The threat model must assess components of the UAS drone (i.e. a network of sensors; navigation system, electronic system, actuators, power system, mainframe, payload and communication links to the environment and the ground control systems).

The capabilities of the adversary can be graded from low, medium to high (Altawy et al. 2016). **Low** is the ability to disclose information (getting access to communication or data stored in unencrypted form). **Medium** is the ability to be authenticated by the UAS system and gaining access to on-board data. **High** is the ability to control or disrupt the regular operation.

Security threats of consumer drones mentioned in Valente (2017) and Altawy et al. (2016). are:

- Fly away attacks (stealing the drone) or Take-down a flying drone - intentionally causing accidents (in sensitive areas as nuclear plants or in national symbols) –through jamming or spoofing the GPS data or the UAS transmissions.
- Injecting falsified sensor data or performing Denial of Service attacks to destabilize the UAS making it to crash.
- Malicious hardware or software, such as backdoors to take control of the system. (A backdoor was also present in Boeing 787, making it possible to take over the avionics and control the airplane).
- Loss of communication - Lock-out owner of the drone from connecting; or manipulating the video streams used to navigate the UAS.
- Steal user data (pictures, streaming video, communication link) and related privacy issues – taking unauthorized video or pictures
- Privacy issues – as an example: drone supplier collects data from flight and stores data in servers in the US and in China

These vulnerabilities are due to several issues, such as lack of authentication (of the operator and devices), poor/ no encryption of communication, poor password protection. These issues can be mitigated as described in Valente (2017) by securing drone access by strong passwords in user authentication; limiting devices allowed to connect (i.e. enforce authentication); disabling services with poor security (Telnet, FTP); encrypting communication, certify software dependent on risk levels and continuously upgrade software in use. A similar set of security requirements are suggested by Altawy et. al. (2016), i.e. only authorized access; specification of availability in operations; information confidentiality and integrity; system integrity i.e. ability to guarantee authenticity of software and hardware components and accountability of actions (i.e. register of issued actions/ commands). These requirements have identified the need for a broader eco-system approach in developing the infrastructure and service environment of drones, as described by Johnsen et al. (2017).

Manned aviation has become highly automated and have reduced the crew from five-person crews in 1950s to two-person crews from 1990s. There is a discussion to reduce crews to single pilot (Driscoll et al. 2017). The main reasons humans are still on the flight deck is to manage risks and handle the unexpected or complex situations. Automation is reliable but computers give up at the first sign of trouble, needing human intervention whether the human is ready for it or not. This creates the need for more understanding and research in Resilience Engineering i.e. the ability to handle the unexpected and recover, (Johnsen et al. 2017).

Some of the challenges of controlling UAS by air traffic controllers are the restricted see-and-avoid capabilities (due to restricted view of airspace); delayed response to instructions since control is dependent on control signals from Ground Control; Differences in size and speed (leads to varying impact of turbulence); extra workload on the operators; (Altawy et al. 2016). These challenges can lead to drone collisions or by drone crashing into the terrain.

Due to the possibilities of mishaps, the quality of safety and security in the UAS software should be certified by an appropriate agent. The range of environments and the differences in UAS operations creates different requirement and risks. A risk-based approach of certification is suggested in Graydon et al. (2009), based on the aircraft, the payload, the mission and the operating environment. In Perez (2012) there is a description of robust autonomy that can be used as a framework for certification, to ensure that the autonomous system can continue its operations or safely shut down. In addition, the security requirements from Altawy et al. (2016) should be a part of this certification scheme.

A more proactive mitigation of attacks by UAS can be established in sensitive areas through monitoring drones by electro-magnetic waves, cameras (heath sensitive cameras recording temperatures or using broader spectrums) or by sound. Then halting or stopping drones through attack drones or jamming as mentioned in Kaleem et al. (2018), Altawy et. al (2016). In addition, there are anti-drone rifles designed to disable drones within 1300 feet, Altawy et al (2016).

Mobile phone applications have also been developed for prison staff, to be able to detect drones crossing into prison areas. More advanced examples of detection and identification of UAS has been done by Quilter et al (2017) using staring radar in Monaco, to identify drones within 5 km distances.

Undesired UAS incidents in urban areas, Pathiyil (2017), are described as:

- Injury to persons, by UAS – a special case could by collisions with manned aircrafts or disruption of air traffic
- Damage to property or to UAS (Theft and vandalism)

- Loss of privacy (physical, emotional, data)
- Sound pollution, disturbances by flying drones in the vicinity of people

Sound pollution from UAS can be significant, in Kloet et al (2017) they found that propeller design and odd number of blades can significantly reduce noise (using experiences from low noise fans). There is a need for legislative restrictions and guidelines to ensure noise to be acceptable.

Systematic documentation of drone incidents (safety and security issues) are needed in order to implement risk-based mitigation, support learning and be able to estimate and improve MTBF.

The risk is dependent on type of operation (delivery, data collection, surveillance, photography, inspection, other…) and details of UAS (weight, speed, height of operation). EASA (2016) has estimated probability of fatality of different UAS weights, and estimated probability of fatality as 1% with an UAS weight of 250g, but 50% fatality with a weight of 600g.

Pathiyil et al (2017) lists UAS safety guidelines from regulatory bodies around the word, describing distances from people, property and safe height limits. Regulation varies, related to densely populated areas: i.e. "do not fly overhead people and property & do not fly within 50 meters of persons and property" from EASA; or "Keep sufficient distance from people and property", from Singapore. Limits are often prescribed (i.e. 30 metres, 50 metres or 75 metres) or based on assessment (i.e. enough distance, safe distance, minimize hazard). Maximum height, are from 200 feet (60 meter) to 492 feet (150 meter). In Ireland UAS flights over populated area can be conducted only at 5000 feet (1500 meter) or higher.

In Norway UAS are divided in three classes with increasing requirements (CAA, 2018):

- RO1: Max weight 2.5 kg. (Operations within line of sight)
- RO2: Max weight 25 kg. (operations under 120 m (400 foot) - if out of sight – restrictions related to rules governing control systems).
- RO3: Weight more than 25 kg may fly 120 m above ground; pilot must have LAPL (Light Aircraft Pilot Licence), PPL (Private Pilot License), CPL (Commercial Pilot License) or ATPL (Airline Transport Pilot Licence). Must communicate with Air Control.

Risk assessment of integrating UAS into controlled airspace has been performed in Ferreira et al. (2018). New hazards are introduced such as probability of collisions, disruption of traffic, loss of communication. There is also a need to establish more rigorous methods to include UAS in urban areas and in shared spaces (i.e. controlled airspace). They found that the risk levels of UAS were acceptable related to defined target level of safety stipulated by ICAO - International Civil Aviation Organization. However, the workload of the aviation controllers must be assessed as UAS are introduced into the airspace.

In Rao et.al (2016) there was a discussion of the societal impact of commercial drones – discussing issues such as damages to persons or property, privacy issues and ownership of data and personal and commercial liability. Mitigating actions were suggested to be a registry of drones and owners, and real-time systems for drone detection in critical areas. To ensure minimal harm, it was suggested that a drone should have the ability to go to a safe/ secure state by perform safe landing (example using a parachute) or travel to a safe site, this is also suggested by Gomes et al (2017). GPS jamming was mentioned, as an attack that may disrupt other vehicles or cause accidents/ collisions. Challenges and mitigation from Rao et.al (2016) are listed in Table 2:

Table 2. Some challenges and mitigating actions

Challenges	**Mitigation**
Privacy detection	Registry of owners/ drones Systems for drone detection
Accountability	Assign liability to owners, Registry of owner/ drones
Control/ Regulation	Drone tracking; Ability to safe landing; Insurance; Definition of aerial bounds;Regulation in sync with technology development

A key issue has been the slow regulatory process as technology is rapidly being developed. In Eurocontrol (2006) a specification is described for the use of military unmanned aerial vehicles as operational air traffic outside segregated airspace. This structure can be explored when establishing functional based rules and regulation.

Management of risks, safety and security should be based on risk frameworks looking at scenarios where UAS is being used. The risks must be managed by taking steps to reduce the likelihood of major hazards (i.e. rules limiting the use of UAS) and reduce the severity (reduce effect of impact, keeping distances from objects that can be damaged). The risk governance framework from Renn (2005) should be used, consisting of problem framing, documentation of hazards and vulnerabilities, risk judgement, risk communication and risk management.

3.3 *Result from interviews*

Key findings from the interviews were the need to explore the conditions and premises of design in relation to the role of the human actors, and to explore and do more research related to how autonomous systems can handle the unexpected.

Related to UAS, the interviews identified several key topics related to maintaining the safety of the future aviation system. Firstly, the

drone industry points out that there are two technological assumptions for future smart drones, namely the development of artificial intelligence integrated aboard the drone, as well as data protocol for communicating with the outside world. The drone industry does not perceive that technology per se will be a major obstacle to future developments.

However, challenges regarding future regulation are pointed out - it is important that in the next few years a common European legislation is put in place that provides more predictability related to the use of UAS. Given the possibilities for drone technology, there are regulatory challenges. Regulation is unable to keep up with technological developments, which makes it challenging to develop practices and thus predict what is coming. This is also due to poor sharing of information of technological progress.

There is a need to establish competence requirements for drone pilots, which minimum requirements should be required? This is important in terms of safety because, apart from knowing that the drone is reliable, one should also be able to trust that the person operating the drone over people have enough competence. The drone industry sees a need to build a safety culture like traditional aviation, since they are newcomers and are conscious/ humble in relation to such a role.

From the drone industry, it is emphasized that the traditional aviation industry must recognize that drone use involves many members who do not have a traditional, aeronautical background, but at the same time are part of the future of aviation. The question is how to work best together. It is a great deal to learn and we are just starting.

4. Conclusions

There are many challenges and opportunities when introducing UAS systems. Some of the benefits or opportunities are:

- The possibility to transfer dangerous operations to drones, minimizing the possibilities of accidents or harm to people. (By moving risky operations to drones).
- The possibility of saving lives in a crisis by getting better information or speeding up delivery of critical supplies (i.e. blood or medicines)
- The possibility to utilize and explore best practices from the ultra-high safety record of manned aviation into the UAS area

Challenges related to establishment of safe and secure UAS operations:

- Research and exploration of the ethical and social aspects of the use of UAS – strengthen and building societal actor networks to work with the issues (i.e. responsible adaption, privacy issues…)
- Research into Human Factors based design of UAS such as Human factors Guidelines for Ground Control centres focusing on conditions and premises of the human actors.
- Increased focus on security and safety of UAS, especially of UAS to be used in an industrial setting focusing on major risks and improvement of MTBF
- More research related to how autonomous systems can handle the unexpected and surprises – and reflections on how to include the human in the loop when almost all functions are automated, and the human must handle the unexpected
- Systematic documentation and reporting of all drone incidents in order to establish systematic data from incidents (safety and security related) and be able to explore MTBF in a systematic manner
- Regulation to support deployment of industrial UAS in urban areas, and to integrate UAS in controlled airspace
- Certification scheme and quality assurance program of requirements for industrial UAS to mitigate safety and security issues
- Building and supporting systematic collaboration between key actors such as regulators, developers, suppliers, users, user organisations (such as UAS Norway) to ensure rapid development of best practices

Acknowledgement

Work with this paper has been funded by the research council through the SAREPTA project

References

Amalberti, R. (2017). The paradoxes of almost totally safe transportation systems. In *Human Error in Aviation* (pp. 101-118). Routledge.

Altawy, R., & Youssef, A. M. (2017). Security, privacy, and safety aspects of civilian drones: A survey. ACM Transactions on Cyber-Physical Systems, 1(2), 7.

Balasingam, M. (2017). Drones in medicine—The rise of the machines. International journal of clinical practice, 71(9), e12989.

Chowdhury, S., Emelogu, A., Marufuzzaman, M., Nurre, S. G., & Bian, L. (2017). Drones for disaster response and relief operations: A continuous approximation model. *International Journal of Production Economics*, *188*, 167-184.

Civil Aviation Authority Norway CAA (2018) https://luftfartstilsynet.no/en/drones/commercial-use-of-drones/about-dronesrpas/regulations-of-drones/

Driscoll, K. R., Roy, A., Ponchak, D. S., & Downey, A. N. (2017, March). Cyber safety and security for reduced crew operations. In Aerospace Conf, 2017 IEEE (pp. 1-15).

EASA and drone rules (2018) - https://www.easa.europa.eu/document-library/opinions/opinion-012018

EASA, Prototype Commission Regulation on Unmanned Aircraft Operations – Explanatory Note, 22 August 2016, Annex 1.

Evjemo, T. E. (2018). Sikkerhet og autonomi i norsk luftfart utfordringer og muligheter. SINTEF Rapport 2018:01451

Eurocontrol (2006). Eurocontrol Specifications for the Use of Military Unmanned Aerial Vehicles as Operational Air Traffic Outside Segregated Airspace- Report Ed. 0.9, Apr.

Ferreira, R. B., Baum, D. M., Neto, E. C. P., Martins, M. R., Almeida, J. R., Cugnasca, P. S., & Camargo, J. B. (2018). A Risk Analysis of Unmanned Aircraft Systems (UAS) Integration into non-Segregate Airspace. In 2018 International Conference on Unmanned Aircraft Systems (ICUAS) (pp. 42-51).

Firesmith, D.G. (2003). "Common concepts underlying safety, security, and survivability engineering", Technical note CMU/SEI-2003-TN-033, Carnegie Mellon University.

Gomes, R., Straub, J., Jones, A., Morgan, J., Tipparach, S., Sletten, A., ... & Miryala, G. (2017). An interconnected network of UAS as a system-of-systems. In Digital Avionics Systems Conference (DASC), 2017 IEEE/AIAA 36th (pp. 1-7). IEEE.

Graydon, P., Knight, J., & Wasson, K. (2009). A flexible approach to authorization of UAS software. In Digital Avionics Systems Conference, 2009. DASC'09. IEEE/AIAA 28th (pp. 5-C). IEEE.

He, D., Chan, S., & Guizani, M. (2017). Drone-assisted public safety networks: The security aspect. IEEE Comm. Mag., 55(8), 218-223.

Hoefer, C, (2003). "Causal Determinism".

Hobbs, A., & Shively, R. J. (2014). Human Factor Challenges of Remotely Piloted Aircraft. In 31st EAAP Conference (pp. 5-14).

Johnsen, S. O., & Stålhane, T. (2017). Safety, security and resilience of critical software ecosystems. ESREL (2017).

Kaleem, Z., & Rehmani, M. H. (2018). Amateur Drone Monitoring: State-of-the-Art Architectures, Key Enabling Technologies, and Future Research Directions. IEEE Wireless Communications, 25(2), 150-159.

Kloet, N., Watkins, S., Wang, X., Prudden, S., Clothier, R., & Palmer, J. (2017). Drone on: A preliminary investigation of the acoustic impact of unmanned aircraft systems (UAS). In 24th International Congress on Sound and Vibration (pp. 1-8).

Lund, J., & Aarø, L. E. (2004). Accident prevention. Presentation of a model placing emphasis on human, structural and cultural factors. Safety Science, 42(4), 271-324

ND (2018) Government White paper "Drone Strategy" www.regjeringen.no/no/dokumenter/norges-dronestrategi/id2594965/

NTSB (2010) - National Transportation Safety Board (Report- NTSB/AAR-10/03).

Parasuraman, R., & Riley, V. (1997). Humans and automation: Use, misuse, disuse, abuse. Human factors, 39(2), 230-253.

Pathiyil, L., Yeo, V. C., & Low, K. H. (2017). Issues of safety and risk management for unmanned aircraft operations in urban airspace. In Research, Education and Development of Unmanned Aerial Systems (RED-UAS), (pp. 228-233). IEEE.

Perez, T., Williams, B., & de Lamberterie, P. (2012). Evaluation of robust autonomy and implications on UAS certification and design. In Proceedings of the 28th Congress of the International Council of the Aeronautical Sciences (pp. 1-9).

Petritoli, E., Leccese, F., & Ciani, L. (2017). Reliability assessment of UAV systems. In 2017 IEEE International Workshop on Metrology for AeroSpace (MetroAeroSpace) (pp. 266-270). IEEE.

Quilter, T., & Baker, C. (2017). The application of staring radar to the detection and identification of small Unmanned Aircraft Systems in Monaco. In Radar Symposium (IRS), 2017 18th International (pp. 1-9). IEEE.

Rao, B., Gopi, A. G., & Maione, R. (2016). The societal impact of commercial drones. Technology in Society, 45, 83-90.

Renn, O. (2005). "Risk Governance – Towards an Integrative Approach" White paper no.1 – International Risk Governance Council.

SAE (2016). SAE International standard "J3016: Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems." Revised: 2016-09-30

Time (2018) - http://time.com/rwanda-drones-zipline/

Vagia, M., Transeth, A. A., & Fjerdingen, S. A. (2016). A literature review on the levels of automation during the years. What are the different taxonomies that have been proposed?. Applied ergonomics, 53, 190-202.

Valente, J., & Cardenas, A. A. (2017). Understanding security threats in consumer drones through the lens of the discovery quadcopter family. In Proceedings of the 2017 Workshop on Internet of Things Security and Privacy (pp. 31-36). ACM.

Waraich, Q. R., Mazzuchi, T. A., Sarkani, S., & Rico, D. F. (2013). Minimizing human factors mishaps in unmanned aircraft systems. Ergonomics in Design, 21(1), 25-32