2020 International Conference on Unmanned Aircraft Systems (ICUAS)
Athens, Greece. September 1-4, 2020

Capability caution in UAV design

Dylan Cawthorne[1] and Arne Devos[2]

Abstract— **Concerns about the impact unmanned aerial vehicles (UAVs) will have on society is growing, making the consideration of ethics in UAV design urgent. Privacy, safety, and security are widely discussed, but engineers have few tools to address these and other ethical issues in their designs. This paper contributes by helping to bridge the gap between ethical theory and design practice. To do so, the concept of capability caution in UAV design is introduced. Capability caution in UAV design is the need for setting well-reasoned limits to the technology's capabilities during the design phase, both to limit risks of misuse, but also to enhance performance within the specified application. Five capability caution design principles are developed which should be considered: 1. context of use 2. privacy 3. jobs and human skills 4. safety, security, and misuse, and 5. the future. A Danish healthcare UAV that has been designed using the capability caution design principles is presented to illustrate the approach.**

I. Introduction

With the increased use of unmanned aerial vehicles (UAVs), or 'drones', in civilian applications, concern is growing about the impact they will have on society [1]. The general public is especially concerned about privacy, safety, and the drone's potential for misuse [2]. Recent literature indicates that acceptance of new drone applications can only be achieved if the ethical implications of the technology are taken into consideration. Reference [3] suggests that *the public good* should be used as a criterion to determine if the drone's use is beneficial. Yet, discussion of what qualifies as the public good is ongoing.

At the same time, legislative bodies try to keep up with this rapidly evolving technology [4]. These new regulations are an attempt to reduce the safety risks of drone operations, like the collision between a drone and a passenger airplane in Quebec City in 2017 [5]. However, even with these efforts, there are concerns over the enforcement of these laws [6], the involvement of lobbying groups [7], and the fact that more complex issues like security and ethics are not well addressed [8].

Engineers often miss the tools or knowledge to address ethical issues in drone design, and thereby address the growing concerns about the technology. Approaches like value sensitive design (VSD)[9] help by identifying stakeholders and their values early in the design process, using these as design inputs. However, VSD is a generalized methodology, and guidelines that are focused on drone design would be useful for those working in the field.

In this work, capability caution in UAV design and five capability caution design principles are developed as an approach to address some of these issues. In so doing, future drones can be more safe, secure, and high-performance within their intended application area.

> *Capability caution in UAV design is the need for setting well-reasoned limits to the technology's capabilities during the design phase*

II. Reading Guide

First, the five capability caution design principles are introduced in section III. In sections IV- VI, important background information about drone capabilities and capability caution is presented. The development of the five capability caution design principles is detailed in sections VII-XI. Established literature and theories from disciplines such as philosophy of technology and value sensitive design are built upon to develop the principles. Potential barriers to the widespread adoption of capability caution are discussed in section XII. Capability caution and the five design principles are demonstrated via a case study of the design of a Danish healthcare drone in section XIII. Finally, in section XIV, potential future work within capability caution in drone design is presented.

III. Capability caution design principles

The drone engineer should consider the design principles listed in Table I early, and throughout the design process. They include consideration of: 1. context of use 2. privacy 3. jobs and human skills 4. safety, security, and misuse, and 5. the future. These principles are guidelines only, and are not exhaustive or a substitute for stakeholder engagement. As identified in [12], it is the process of developing drones, including engagement with members of the public, that makes it fair - not only the resulting product. Thereby, 'to shift away from the current focus on citizens' acceptance of civil drone development towards the development of civil drones that are acceptable to citizens'.

IV. Drone Capabilities

Drones have their origin in a military context, where they perform surveillance tasks and precision combat [13].

[1]Dylan Cawthorne is with the Unmanned Aerial Systems Center at the University of Southern Denmark, Campusvej 55, 5230 Odense M, Denmark dyca@sdu.dk

[2]Arne Devos is with the Mærsk Institute at the University of Southern Denmark, Campusvej 55, 5230 Odense M, Denmark ardev18@student.sdu.dk

TABLE I

THE FIVE PRINCIPLES FOR CAPABILITY CAUTION IN DRONE DESIGN

Design Principle	Approach	Questions to consider	Reference
Principle 1: Consider the context of use	Focused design should be the default Avoid 'universal' or 'one-size-fits-all' solutions Design for a specific context of use Design for a precise use-plan Minimize the drone's ability to be used outside the intended context of use or use-plan Identify and address potential dual-use issues	How can the drone be designed for the specific context of use? How can the drone be designed for the precise use plan? How can the risk of dual-use be minimized?	Section VII
Principle 2: Consider privacy	Follow the seven privacy by design principles [10] Adhere to the seven General Data Protection Regulation principles [11] Select the drone's sensors and design the data processing so as to preserve privacy (Fig. 1) Minimize the drone's 'invisibility' and ability to spy (or to be *perceived* to be spying)	How can the drone design prevent privacy violations? Is more data being collected than is needed? Is the drone highly visible and audible to reduce spying?	Section VIII
Principle 3: Consider jobs and human skills	Consider what type and level of automation the drone should possess Decide what work should be automated, such as dangerous tasks, and what work should be performed by humans, such as life-critical decisions, human interaction, and creativity Carefully manage the impact to the existing workforce	How can the drone be designed to enhance meaningful human work? How can the drone's design minimize negative impacts on the existing workforce?	Section IX
Principle 4: Consider safety, security, and misuse	Carefully define upper limits to the drone's capabilities such as payload, range, weight, speed, and geographical operating boundaries Maximize the difficulty by which the drone could be used to carry unapproved cargo such as a bomb or viral weapon Limit the ability of the drone to be crashed into manned aircraft, people on the ground, or critical infrastructure Note: it might not be possible to prevent all misuse, but the aim is to make it as difficult as possible	How can the drone's ability to carry dangerous or illegal cargo be reduced? How can the design limit the likelihood and severity of consequences if it falls into the wrong hands or is hijacked?	Section X
Principle 5: Consider the future	Avoid that the drone's design will lead to or facilitate undesirable drones in the future Clearly define the upper limits to the required functionality Be cautious of over-specification based on possible future scenarios that are not yet part of the design requirements	What will be the long-term impact of developing this drone? Has the drone been over-specified? Should this drone be developed at all?	Section XI

Military drones require capabilities that allow them to excel at these tasks - capabilities such as survivability, invisibility, and remote sensing [14]. Civil drones require different capabilities. For example, an agricultural drone used to monitor crops will also require remote sensing, but will not require survivability or invisibility. In an agricultural context, survivability is not required as the drone is not under attack. Invisibility is not required either, and could actually be detrimental to its function. An 'invisible' drone in an agricultural setting might be considered a spy drone and risk privacy violations. Therefore, different specifications are required for drones in civil use than in military use, both for ethical and performance reasons.

A. Drones as Platforms

Drones are often described as platforms, both in academic literature [15] [10] [16] and by drone manufacturers [17] [18]. They are positioned as flying multi-tools which can carry anything; 'in the commercial space, drones are viewed as platforms for sensors of any kind' and 'currently, there is not regulation that controls the payload that is carried on the drones' [1]. The term platform is being used in the discourse around online content providers such as YouTube as well [19] where it is used to signify a morally neutral technology that simply provides users with the ability to express themselves. Yet, content providers paradoxically seek protection for facilitating user expression, while at the same time seeking limited liability for what users say [19]. Drone technology is in a similar position - the flexibility of the technology is promoted, but limited responsibility is taken for the payload or how the drone is used. The non-morally-neutral character of technology - that technology supports certain actions and thereby has moral importance - is widely accepted within the philosophy of technology [20]. Therefore, drone engineers, researchers, and manufacturers must take an active role in the appropriate specification of the technology, and accept at least some responsibility for the use (and misuse) of their products. Capability caution in

drone design provides an approach which can help them do so.

V. Capability maximization

Capability maximization and the ideal of an optimal design are often the default approaches in engineering contexts. However, there are alternative strategies. One such approach, which is especially relevant in a discussion of capability caution, is *satisficing with moral obligations* [21]. 'In contrast to an optimizer, a satisficer does not look for the optimal option but first sets an aspiration level with respect to the options that are good enough and then goes on to select any option that exceeds that aspiration level' [21]. For example, rather than optimizing the drone's environmental impact, the acceptable level of impact for the context of use is determined and, once this threshold is met, any design that meets this level is considered acceptable. Determination of the acceptable threshold is critical in such an approach. Satisificing with moral obligations ensures that the threshold does not violate moral considerations. It has been argued that moral thresholds are context-dependent and that, for example, the minimum moral standard for environmental impact in a society of abundance would be different than in a society of scarcity [21].

VI. Capability Caution in Design

Capability caution in design has been a topic of interest most recently within the field of artificial intelligence (AI) [22]. AI could soon become very powerful, with capabilities that are currently hard to imagine. In addition, since it is still being developed, it is not possible to know exactly where the evolution of AI technology will lead. This means that the risks of AI could be significant and unpredictable. Therefore, those in the AI community argue that it must be pro-actively developed 'within secure constraints'[22] - utilizing capability caution. The general problem of not knowing how a new technology will impact society until it has already begun to do so is called the Coolingridge Dilemma, and has been discussed at least since 1980 [23]. The concepts of capability caution and the Coolingdrige Dilemma also apply to the drone domain. Drones could utilize AI, making capability caution directly applicable. Even without AI, drones are a powerful and unpredictable technology, with a significant potential for misuse, and whose eventual impact on society cannot be known.

Capability caution in drone design can be conceptualized on different levels. At a macro level, it means consideration of the future - the long-term, far-reaching implications of the technology on society. It asks engineers to consider what their work today will facilitate in the future, and if certain drones should be developed at all. Then, they can pro-actively design (or not design) drones which lead to a better future. These ideas are explored further in section XI. Proper specification requires an understanding of the drone's intended context of use and use-plan, discussed in section VII.

At a micro level, capability caution means setting well-reasoned limits on the drone's specific functions to increase its performance and reduce the chances of misuse. This includes choosing sensors which protect privacy (section VIII) and designing autonomy to minimize disruption to the workforce and increase the availability of meaningful work (section IX). It includes consideration of the drone's size, weight, speed, shape, maximum payload, and maximum range, which impacts safety, security, and misuse (section X). A pro-active approach to capability caution means less resources are required to defend against 'rogue drones' [24] [25], and more trust is engendered in the technology.

In the following five sections, these considerations, which have been divided into five capability caution design principles, are developed, justified, and explained.

VII. Principle 1: Context of use

Drones are designed to be operated, not in a 'vacuum', but in the world. Therefore, consideration of the physical and social context where they will be deployed - their context of use - is critical. The task of the drone engineer is to understand this context and design a product that fits well within it. For example, a drone that will be operated in Antarctica to map sea ice will have different functional requirements with regards to operating temperature than one designed to transport blood in Africa. As well, the laws, social norms, and perception of drones will differ in the two locations - a drone that is like a 'flying donkey' [26], could be perfectly suited to Africa, but not necessarily to Antarctica.

Another task of the engineer is to determine how the drone should be operated - the use-plan. The drone and the use-plan are often developed in parallel, where the technology and the way it will function influence one another. The use-plan can be explicit, such as a user manual or instructional video, and/or implicit, and influenced by the way the system is designed. The use-plan for a drone that maps sea ice and a drone that transports blood will differ significantly. Designing a drone for a specific context of use and use-plan can be facilitated by engaging with stakeholders, as described in the next subsection VII-A.

A. Stakeholders

Drones impact many people, organizations, animals, and the environment during their design, production, operation, and end-of life. Those who are impacted are called stakeholders, and they can be divided into direct stakeholders - those that interact directly with the technology, and indirect stakeholder - those that do not interact directly with the technology, but are still affected [9]. Methods within the value sensitive design (VSD) literature provide guidance on how to identify and gather inputs from stakeholders [9]. Unlike traditional stakeholder influence mapping, the VSD approach suggests that not only powerful stakeholders inputs should be considered. The general public are an often overlooked stakeholder group. Sometimes, technology is forced upon them in the hope that they will come to accept it, or with the belief that they have no other choice

than to accept is. 'At present, the burden of acceptability is with the citizen, the target of information actions that are designed to transform them from the passive role of opponent to the passive role of acceptor' [12]. Responsible drone engineers engage with and consider their technology's impact on stakeholders, irrespective of that stakeholder's power or influence.

B. Dual-use

As discussed in section IV, drones have significant history within a military context of use. The term 'dual-use' is used to describe a (drone) technology that could be used both in a military and a civil context. However, it should be noted that it can be difficult to draw a strict line between military and civil uses, such as drones for border security [27] or police work [14], which require many of the same (but not identical) capabilities as those for military reconnaissance [28]. In addition, the boundary between the domains is quite permeable, with military and civil drones benefiting from developments within the other field. For example, the Cumulus, a civil drone originally developed for agriculture and 3D mapping, has been made into the Heidrun, a military drone for reconnaissance and tactical engagement [18].

Dual-use leads to practical limitations in the sale and movement of drone technology. The European Union exercises control over the export, transfer, and transit of dual-use items via Regulation 2016/0295 [29]. This includes drones that can fly beyond the visual line of sight of the operator and have a maximum endurance over one hour. Capability caution in the design, such that the drone does not surpass these criteria, means it can be sold and transferred between EU member states without restriction.

Dual-use is sometimes defined in terms of a technology or research that can be used both for good and bad purposes; this general problem is referred to as the dual-use dilemma [30]. Reference [28] sites four ethical principles that can be applied to the dual-use dilemma. One is that of collective responsibility: 'the responsibility for the research, technology, or artefacts cannot be carried by the individual scientist alone, relying exclusively on one's self-governance. The responsibility is a collective effort on multiple levels, and it is a joint enterprise of universities, professional associations, governments, and funders' [28]. However, the shared nature of responsibility does not preclude the drone engineer from actively trying to reduce the risks of dual-use while creating technology, and the implementation of capability caution can aid in this endeavour.

VIII. Principle 2: Privacy

Privacy concerns associated with the use of drones have been widely discussed [31] [32]. However, in a case study [12], developers and researchers stated that it was too hard to predict how privacy would be situated in a certain context while the drone was still in the development phase. As a result, protecting privacy was not seen as a priority. The developers argued that they adhered to legal requirements, and that privacy would have to be considered while integrating the system into its context.

TABLE II
The privacy by design guidelines with drone examples

Privacy by design guideline	**Examples for drone design**
Taking a proactive rather than reactive approach	Make it clear through markings on the drone when there is no camera so individuals do not feel spied on
Privacy as default setting	Camera gimbal prevents pointing the sensor into the neighbor's yard
Embedding privacy in the design	Facial blurring happens in the camera module and can not be turned off
Aiming for full functionality while maintaining privacy	If a camera is only needed for landing or guiding, no images are stored or transmitted
Ensuring full life-cycle protection of sensitive data	Collected data is encrypted and automatically destroyed once it fulfilled its purpose
Visible and transparent operations	Inform when and why the drone is filming through an app, or lights and sounds that come from the drone
Taking a stakeholder-inclusive and user-centric approach	Engage with the stakeholders through focus groups and workshops

The European Union's General Data Protection Regulation (GDPR) [11] can provide guidance in pro-actively designing for privacy. While required in the EU, the GDPR can also be used to inform privacy-aware drone designs in other locations. The GDPR lists seven guidelines that need to be implemented to protect data and privacy. Data should be collected *lawfully, fairly, and transparently*. *Purpose limitation* should be observed; data that is collected for a specific purpose should only be used for that purpose. *Data minimisation* refers to only collecting data that is absolutely necessary. The data must be *accurate*, kept up to date, and erased or modified if inaccurate. *Storage limitation* means that data should only be stored for as long as necessary. All data has to be protected from unauthorized access or unlawful processing. This is called *integrity and confidentiality*. The last guideline is *accountability*. The responsible parties should do their best to comply with all the other principles, and accept collective responsibility for the enactment of the regulations.

Privacy by design guidelines that apply directly to drones were proposed in 2012 [10]. They are listed in Table II, along with examples of technological choices a drone engineer might utilize to conform to them. Smart routing of drone flight paths could also enhance privacy - it would ensure that the drone would not overfly areas marked as private [31]. Citizens would be able to make their privacy preferences known, and choose to accept drone operations over their property, disallow operations, or allow them on a contextual basis, such as during a police emergency.

Fig. 1. Privacy by design and data minimization can be realized with automatic, algorithmic blurring of faces (image modified by the authors; original from [33])

IX. Principle 3: Jobs and human skills

Drones are part of what has been called the fourth industrial revolution [34] - technologies that have the potential to change the way people in the society live and work [35]. It has been estimated that 47% of jobs in the United States are at risk of being automated [36]. Some jobs are more likely to be automated with drones, such as food or postal couriers [37], field surveyors [38], and security guards [39]. The introduction of technologies can create new jobs, but these jobs are often occupied by employees with a high levels of education like mechanical engineers and software engineers [40].

Implementing a drone often replaces existing work, such as postal deliveries by mail couriers. If automation in the postal service takes place, some or all postal delivery jobs may become obsolete. In return, these jobs might be replaced by office jobs where employees manage a drone fleet from a distant location. This would change what it means to be a mail courier, but might also have other effects on society. Elderly people sometimes rely on the mail courier for social contact. Some countries even offer services where the mail couriers visit people on their delivery route [41]. There is value not only in the delivery of mail, but in the human interactions that takes place, and this must be considered when deciding to automate a job.

Specifying the the type and level of autonomy the drone has will have has a direct impact on the type of work that the operators and support staff will perform. For example, if the flight will be fully autonomous but the operator must monitor the flight for safety reasons, the job may become very boring. Research shows that the main factor for determining if a job is good, is if the job is seen as interesting [42]. Having a drone with a lower degree of automation could actually result in better jobs. A general aim could be to design the system such that it leads to meaningful human work, where people get to make important decisions, be social, and be creative.

X. Principle 4: Safety, security, and misuse

A. Safety

Safety is an area where drone engineers, lawmakers, and the drone industry have focused a lot of attention. Drones can weight tens or hundreds of kilograms, and may be flying over public ground. This means that if something goes wrong, there is a risk to humans, animals, and property [43].

A major factor in determining the severity of injury if a drone hits someone on the ground is its impact energy - limiting the drone's mass and velocity reduces its impact energy and increases its inherent safety. Studies have estimated the amount of energy that the human head, thorax, and abdomen can sustain without serious injury at between 25 joules [44] and 200 joules [45]. Furthermore, it has been estimated that drones under 250 grams can be considered 'harmless' [44], while drones over around 2 kilogram are capable of causing a fatality [45]. Designing the drone so that it is blunt and frangible can also reduce injury if hitting a person [45].

Drones also risk hitting manned aircraft, or being sucked into jet engines [46]. Components, especially high-density and hardness components such as motors and batteries, are unlikely to cause catastrophic damage to a jet engine if their weight is kept below 300 grams each [46].

Capability caution - limiting sensors to only those required in data-collecting drones, and not over-specifying the payload capacity in a cargo drone, reduces the overall weight and increases inherent safety. Limiting the drone's geographical operating boundaries with a geofence to keep it within safety corridors can further reduce the likelihood of injuries or fatalities. The drone can also be equipped with an active fail-safe system, such as an airbag or parachute.

Legislation can be seen as a type of non-optional capability caution - the engineer is forced to restrict the capabilities of the system to enhance safety. European legislation states that drones should be at least as safe as manned aviation, with ten-million flight hours between fatalities [47]. Before a drone operation is allowed, a Specific Operation Risk Assessment (SORA) [48] may be required. The drone's design factors into the assessment, with smaller and lighter weight drones placed into lower risk classes - a lower risk class is 'rewarded' with lower operational safety requirements.

B. Security

Security risks lay in the unauthorized and intentionally maleficent use of the system by third parties. Access to the system by unauthorized people before take-off can be reduced with the use of identification tools; for example, the drone could designed so it can only be launched by a person with the correct credentials. Cargo drones could be designed in such a way that the motor will not operate if the authorized cargo is not locked into the cargo bay.

While the drone is in the air, the main vulnerabilities lay in spoofing of the GPS signal and hacking the communication links. Measures to improve the security can be taken, such as encrypted communications, and legitimisation of the signal source [49]. In the event of a compromised system, a drone

with fewer capabilities could reduce the severity of negative outcomes. The implementation of a geofence would limit the security risks by steering the drone out of restricted areas such as those surrounding airports, government buildings, and, potentially, private properties [31]. If the drone violates the geofence for too long, an independent secondary system could cut the power and deploy an airbag or parachute to bring the drone down relatively safely. Like locking up a bicycle to reduce the chances it is stolen, actively addressing security risks may not prevent all violations, but these actions at least becomes much more difficult to accomplish.

Many countries have enacted outright bans on all commercial drone activities, or have effective bans which means it is not practically possible to get the required permissions to operate [50]. Security risks may play a factor in these outright or effective bans, and drones designed with capability caution in mind might one day be accepted by these countries.

C. Misuse

Misuse can be characterized, not necessarily as intentionally maleficent as in security violations, but following a use-plan that is different than the one invented by the engineer. These uses may be seen as harmless, and may not be performed with bad intentions. This practice is called *innovative using* or *multi-stability* [51]. An example of innovative using or multi-stability would be using a drone as a cooling fan on a hot day.

Misuse, innovative use, or multi-stability can be eased or made more difficult in the design phase. For example, if a drone is easily adaptable, such as a modular drone [52], it will be straightforward to build a configuration which can be used for all types of activities, both beneficial and harmful. Limiting the capabilities of the system limits the possibility for uses that diverge from the intended use-plan.

XI. Principle 5: Consider the future

The future is impossible to predict, but drone engineers can still consider possible future scenarios to help them make better design decisions today. A key future risk, especially within the development of 'drones for good' [53], is the possibility of function creep [54]. Function creep means 'that civil drones may be introduced on the basis of applications with far reaching social benefits, before being extended beyond this mandate for frivolous applications that were not originally envisaged and are not considered acceptable' [54]. For example, introducing medical drones to rapidly transport life-saving defibrillators or urgent medical supplies, followed by the introduction of less beneficent or time-critical applications, such as advertising, coffee deliveries, or police patrols [55].

A similar, but shorter-term, risk is specification creep. This occurs when specifications expand over time, or additional 'future requirements' are considered that are not part of the design space. For example, when a cargo drone is initially designed to transport a small payload over a limited distance, but, with time, the requirements expand so that the drone should carry larger cargo over longer distances. Specification creep can also happen in data collecting drones, leading to the collection of unnecessary personal data and hampering privacy by design (section VIII).

Limiting function creep and reducing the chances that the drone's design will lead to undesirable drones in the future is especially challenging. However, engagement with stakeholders, knowledge of the context of use and the use-plan, along with consideration of capability caution can assist in tackling these complex issues. Prototype testing in the context of use, focus groups with stakeholder, etc., can be used to inform future developments of the design. Finally, choosing *not* to develop a drone is always an option.

XII. Potential barriers to adoption

There are many potential barriers to widespread adoption of capability caution in drone design. It may cost more to develop unique drones that are specially suited for their context of use. Economies of scale favor standardized products as they are less expensive to manufacture. This drives drone manufacturers to use the same platform for both military and civil uses, and develop them with no specific context of us in mind. Flexible manufacturing systems such as in Industry 4.0 [56] could facilitate customized products while still keeping costs down. These drones could be defined using parametric functions to easily generate their shape using computer aided design tools, in conjunction with flexible autonomous manufacturing methods. Although it might not be less expensive, the process of customized manufacturing could be performed manually, as it requires creativity and problem solving - work humans are good at and which they may find meaningful. Either way, the resulting drones would not be one-size-fits-all platforms, but products with focused capabilities that address the context of use and the specified use-plan.

There is a possibility that capability caution will stifle innovation, and that its products would not be successful in the marketplace. Capability caution is not currently common practice in the industry (perhaps with the exception of privacy and safety considerations) where maximization or optimization is considered the ideal. However, this could represent an opportunity to develop technology in a different way and could lead to different, innovative solutions that achieve market success. For example, the US Department of Homeland Security put out a tender for airport body scanners in the early 2000's [57]. Many companies proposed solutions with extremely high-resolution scanning, which resulted in detailed images of people's naked bodies. One company identified that privacy was critically important, and, unlike their competitors, developed a system that identified potential contraband, and overlaid this onto a cartoon version of a human body. This company won the tender; their technology was able to perform as required, while maintaining peoples' privacy and self-respect.

Capability caution could lead to longer development times since many different drone configurations will be required. However, it is a possibility that development of each drone

Principle 1: Context of use
- Danish text on the drone
- Colors like a Danish ambulance

Principle 2: Privacy
- No cameras or privacy-violating sensors
- "No camera" icon on nose
- No personal data on patient samples

Principle 3: Jobs and human skills
- One pilot per drone
- Limited automation
- Minimal impact on existing jobs

Principle 4: Safety, security, and misuse
- Small size and low weight (under 1.5 kg) for inherent safety
- Geo-fencing
- Motor disabled until the blood sample is locked in the cargo bay

Principle 5: The future
- Minimal payload capacity for one blood sample - 85 grams
- Minimal range of 25 km
- Healthcare drones may lead to less desirable cargo drones in the future
- Testing of the prototype will determine if the project should continue

Fig. 2. The proposed Danish blood sample transportation drone incorporates the five capability caution design principles (graphic by the authors)

will be faster than usual because the scope will be focused - rather than attempting to design one drone for everyone and everywhere, the design space will be more limited.

It could be argued that there is no need to adopt capability caution until is becomes legally required. However, responsible design and engineering practices do not rely on legal requirements to set minimal ethical boundaries. New standards and certification programs indicated that more widespread adoption of ethically-informed and capability cautious design practices are on the way. These include the IEEE P7000-series [58], which is a 'process model by which engineers and technologists can address ethical consideration throughout the various stages of system initiation, analysis and design', and the ethics certification programs for autonomous and intelligent systems [59]. Early adopters will be well prepared when the standards come, and ahead of their competitors in development.

Widespread adoption of capability caution in drone design could facilitate a shift in responsibility away from users to engineers and designers. Since engineers and designers take a more active role in the specification of the drone for use in a specific context, the user's ability to decide where and how to operate the drone will be reduced. For example, a drone that is geo-fenced reduces the user's ability to fly anywhere they like. But, the geo-fence will also prevent the user from (intentionally or unintentionally) flying too close to an airport, increasing the safety of the system. It could be argued that reducing a user's ability to operate a drone in an unsafe manner actually enhances the functionality of the drone, since it is easier to use safely. Still, users may be most familiar with highly flexible technologies and be less accepting of those that limit use-plans. Producers could make it possible to bypass some restricting features provided users present the necessary approvals For example, operators that have permission from an airport to use a drone to scare birds off the runway could be given special permission and bypass the geo-fence.

XIII. Capability Caution in the Design of a Danish Healthcare Drone

In this section, the case of a Danish healthcare drone utilizing the five capability caution design principles is presented to illustrate their application.

The Danish healthcare system is in the midst of a move towards centralization and specialization of hospitals and equipment, reducing the number of hospitals with 24 hour care from 41 to 20 [60]. As a result, expensive advanced blood sample testing equipment may be located at another facility. The HealthDrone project [61] aims to reduce cost, increase speed of delivery, and improve environmental sustainability using drones to transport blood samples. The proposed drone design, shown in Fig.2, is an attempt to satisfy the design objectives while utilizing the five capability caution design principles.

A. Principle 1: Context of use

Denmark has a robust infrastructure, and driving between hospitals is easily accomplished. However, access to some of the island communities is more challenging. It was determined that the most urgent case for medical sample transportation by drone, and where independence of the local population could be enhanced, was the route from the island of Ærø to the city of Svendborg - a straight-line distance of 25 km mostly over the ocean. Here, ferry service limits the speed and flexibility of transportation of samples off the island. Additionally, urgent samples were identified as the most critical - the drone could be seen as a 'flying ambulance'. It was designed specifically for a context of use - the island of Ærø, and a specific use-plan - to transport urgent samples.

B. Principle 2: Privacy

The privacy by design guidelines [10] have been followed - the drone does not use sensors which capture personal data, and the patient's samples are made anonymous to protect their privacy. There is currently no generally accepted symbol

which demonstrates that a drone does *not* have a camera on it, so for now an icon of a camera with a slash through it is used, as shown in Fig. 2.

C. Principle 3: Jobs and human skills

The widespread use of healthcare drones will lead to a shift in the number and types of jobs available across Denmark, and therefore the types of human skills that may be in demand. The practice of delivering samples from one hospital to another may seem straightforward, but the task also includes taking responsibility for a potentially dangerous biological substance that contains peoples' DNA. Therefore, continuous monitoring of the drone and its payload is part of the proposed HealthDrone's design. It will operate at a very low level of autonomy. The operator manually flies the drone during launch, cruise, and landing, with one operator per drone. This prevents the operator from being overloaded if there is an incident with multiple drones at once, and fulfills the current legal requirement that each drone have one dedicated safety pilot [62].

D. Principle 4: Safety, security, and misuse

The cargo bay is specially designed to prevent misuse and errors. The drone's motor will only engage when the correctly shaped sample is placed in the cargo bay, and there is only space for the specified samples rather than a large, empty box or cargo pod. This prevents the drone from being launched if the operator forgets to load the sample, and reduces the ease at which non-approved cargo can be carried inside the drone. Once the samples are inserted, the cargo bay is locked and cannot be opened except by authorized hospital personnel at the receiving hospital. This prevents the sample from being stolen or tampered with during the flight should the drone be intercepted or crash en route.

The drone is GPS-enabled, and a geo-fence prevents accidental fly-aways and misuse. Its software allows it to be launched from the approved hospital's GPS coordinates, fly within pre-defined safety corridors avoiding highly populated and natural protected areas, but not outside of these limits. The geo-fence also prevents the drone from flying too high (over 120 meters within cities and over 100 meters outside of cities). Should the pilot steer the drone off course, the flight path is automatically corrected to stay within the approved flight zone. It cannot be flown over airports, government buildings, or important infrastructure, reducing the possibility of misuse.

E. Principle 5: The future

Mitigating specification and function creep was a challenge in the project. The drone's payload capacity was carefully defined as 85 grams. This includes two blood samples of 10 mL each, packaging as specified under United Nations Regulation UN3373 [63], and the required temperature logger. The drone could have potentially been used to transport larger and heavier payloads such as blood cultures, or blood bags which come in one kilogram sizes, or non-acute (non-urgent) samples. The temperature storage requirements of the payload was defined as 1-35 degrees C. This range is sufficient for (acute) blood samples; again, other payloads having different or more strict requirements, such as plasma which must be kept frozen, would have required increased capabilities. With the carefully defined payload weight and storage temperature requirements, a small, lightweight, and less expensive drone was possible. The focus on acute samples meant that the most critical cases would be delivered more rapidly, but impact on the existing transportation system would be minimized.

The drone's required range also needed to be defined. Again, function and specification creep was a risk with the expanded range of the newest drone designs. Routes from Svendborg to Odense (45 km over land), and Copenhagen to Odense (140 km over land and water) could have been technically possible, but were deemed outside the specified context of use. In the future, a family of Danish healthcare drones could be developed, each with unique capabilities that match their intended use. For example, a standardized shape and overall aerodynamic configuration could be utilized, but various versions could be created, such as a larger version for the longer route between Svendborg and Odense, larger payloads such as blood bags, or a drone with a temperature-regulating payload bay. The result would be drones possessing the desired capability for each use-case, and a reduced risk of misuse.

XIV. Future work

The next-steps will be to test the drone and the capability caution design principles in the real world. A prototype of the drone proposed in the case study is currently being built and will be tested in Denmark. The prototype drone will allow testing of various aspects of the design, including the typical performance criteria such as speed, range, and cost, as well as capability caution-focused criteria such as payload bay security, impact on jobs, and the overall usefulness of a task-specific drone. These inputs will be used to further develop the drone - or as justification to stop the project - as well as to develop the capability caution approach and design principles. For example, some quantifiable criteria by which capability caution can be assessed may be created.

Some of the most compelling open questions within capability caution in drone design are the potential shift in responsibility from users to engineers (section XII), and questions about the future and function creep (section XI) - if engineers' work today will lead to undesirable drones in the future. These questions will need to be addressed with multidisciplinary teams with insight into the relevant philosophical, ethical, social, and technical aspects.

Ideally, other drone researchers and drone companies will see the value of capability caution, and adopt the approach. Then, more real-world feedback can be gathered, and the design principles can be refined over many different applications and contexts of use. Eventually, it could become standard practice for engineers to consider capability caution in drone design.

REFERENCES

[1] B. Rao, A. G. Gopi, and R. Maione, "The societal impact of commercial drones," *Technology in Society*, vol. 45, pp. 83–90, 2016.

[2] B. Aydin, "Public acceptance of drones: Knowledge, attitudes, and practice," *Technology in Society*, vol. 59, p. 101180, 2019.

[3] A. Choi-Fitzpatrick, "Drones for good: Technological innovations, social movements, and the state," *Journal of International Affairs*, vol. 68, no. 1, p. 19, 2014.

[4] C. Stöcker, R. Bennett, F. Nex, M. Gerke, and J. Zevenbergen, "Review of the current state of uav regulations," *Remote sensing*, vol. 9, no. 5, p. 459, 2017.

[5] CBC-News, "A first in canada: Drone collides with passenger plane above quebec city airport," 2017, [Online]. Available: https://www.cbc.ca/news/canada/montreal/garneau-airport-drone-quebec-1.4355792. [Accessed March 1, 2020].

[6] S. French, "Only one drone pilot has ever been busted for flying without a license — and he got a warning," *MarketWatch*, 2018, [Online]. Available: https://www.marketwatch.com/story/exclusive-only-one-drone-pilot-has-ever-been-busted-for-flying-without-a-licensehe-got-a-warning-2018-02-08. [Accessed March 1, 2020].

[7] W. Yakowicz, "Amazon has spent nearly $10 million lobbying for drone delivery," *Inc.com*, 2016, [Online]. Available: https://www.inc.com/will-yakowicz/amazon-spends-millions-lobbying-drone-delivery.html. [Accessed March 1, 2020].

[8] N. Ahmad, "The eu's response to the drone age: A united sky," 2019, [Online]. Available: https://blogs.prio.org/2019/09/the-eus-response-to-the-drone-age-a-united-sky. [Accessed March 1, 2020].

[9] B. Friedman and D. G. Hendry, *Value sensitive design: Shaping technology with moral imagination*. Mit Press, 2019.

[10] A. Cavoukian, *Privacy and drones: Unmanned aerial vehicles*. Information and Privacy Commissioner of Ontario, Canada Ontario, 2012.

[11] EU, "Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data," 2016, [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj. [Accessed March 1, 2020].

[12] P. Boucher, "Domesticating the drone: the demilitarisation of unmanned aircraft for civil markets," *Science and engineering ethics*, vol. 21, no. 6, pp. 1393–1412, 2015.

[13] P. J. Springer, *Military robots and drones: a reference handbook*. ABC-CLIO, 2013.

[14] A. Van Wynsberghe and M. Nagenborg, "Chapter 8: Civilizing drones by design," *Drones and Responsibility: Legal, Philosophical and Socio-Technical Perspectives on Remotely Controlled Weapons*, p. 148, 2016.

[15] B. Vergouw, H. Nagel, G. Bondt, and B. Custers, "Drone technology: Types, payloads, applications, frequency spectrum issues and future developments," in *The Future of Drone Use*. Springer, 2016, pp. 21–45.

[16] R. L. Scharf, "Drone invasion: Unmanned aerial vehicles and the right to privacy," *Ind. LJ*, vol. 94, p. 1065, 2019.

[17] DJI, "Dji website," [Online]. Available: https://www.dji.com. [Accessed March 1, 2020].

[18] Sky-Watch, "Sky-watch website," [Online]. Available: https://www.sky-watch.com. [Accessed March 1, 2020].

[19] T. Gillespie, "The politics of 'platforms'," *New media & society*, vol. 12, no. 3, pp. 347–364, 2010.

[20] L. Winner, "Do artifacts have politics?" *Daedalus*, pp. 121–136, 1980.

[21] I. Van de Poel, "Values in engineering design," in *Philosophy of technology and engineering sciences*. Elsevier, 2009, pp. 973–1006.

[22] L. Floridi, J. Cowls, M. Beltrametti, R. Chatila, P. Chazerand, V. Dignum, C. Luetge, R. Madelin, U. Pagallo, F. Rossi *et al.*, "Ai4people—an ethical framework for a good ai society: opportunities, risks, principles, and recommendations," *Minds and Machines*, vol. 28, no. 4, pp. 689–707, 2018.

[23] D. Collingridge, *The Social Control of Technology*. London, UK: Frances Pinter, 1980.

[24] D. Peri, "Expanding anti-uavs market to counter drone technology," *CLAWS Journal Winter*, pp. 152–158, 2015.

[25] Rafael-Advanced-Defense-Systems-Ltd., "Rafael's drone dome intercepts multiple maneuvering targets with laser technology," 2020, [Online]. Available: https://www.rafael.co.il/press/rafaels-drone-dome-intercepts-multiple-maneuvering-targets-with-laser-technology. [Accessed March 1, 2020].

[26] T. Jackson and M. Wall, "Can 'flying donkey' drones plug africa's transport gap?" *BBC-News*, 2015, [Online]. Available: https://www.bbc.com/news/business-30895278. [Accessed March 1, 2020].

[27] R. Jones and C. Johnson, "Border militarisation and the re-articulation of sovereignty," *Transactions of the Institute of British Geographers*, vol. 41, no. 2, pp. 187–200, 2016.

[28] P. Novitzky, B. Kokkeler, and P.-P. Verbeek, "The dual use of drones," *Tijdschrift voor veiligheid*, vol. 17, pp. 1–2, 2018.

[29] EU, "Regulation 2016/0295 control of exports, transfer, brokering, technical assistance and transit of dual-use items," 2016, [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016PC0616. [Accessed March 1, 2020].

[30] S. Miller, *Dual Use Science and Technology, Ethics and Weapons of Mass Destruction*. Springer, 2018.

[31] P. Blank, S. Kirrane, and S. Spiekermann, "Privacy-aware restricted areas for unmanned aerial systems," *IEEE Security & Privacy*, vol. 16, no. 2, pp. 70–79, 2018.

[32] R. L. Finn and D. Wright, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications," *Computer Law & Security Review*, vol. 28, no. 2, pp. 184–194, 2012.

[33] pxfuel, licensed under CC0, [Online]. Available: https://www.pxfuel.com/en/free-photo-jevsa. [Accessed March 1, 2020].

[34] K. Schwab, *The fourth industrial revolution*. Currency, 2017.

[35] D. M. West, "What happens if robots take the jobs? the impact of emerging technologies on employment and public policy," *Centre for Technology Innovation at Brookings, Washington DC*, 2015.

[36] C. B. Frey and M. A. Osborne, "The future of employment: How susceptible are jobs to computerisation?" *Technological forecasting and social change*, vol. 114, pp. 254–280, 2017.

[37] D. Borščová and K. Draganová, "Utilization possibilities of unmanned aerial systems in postal and parcel services," *Acta Avionica*, vol. 16, no. 2, 2014.

[38] J. Zhang, J. Hu, J. Lian, Z. Fan, X. Ouyang, and W. Ye, "Seeing the forest from drones: Testing the potential of lightweight drones as a tool for long-term forest monitoring," *Biological Conservation*, vol. 198, pp. 60–69, 2016.

[39] Nightingale-Security, "Robotic aerial security," [Online]. Available: https://www.nightingalesecurity.com. [Accessed March 1, 2020].

[40] M. McNabb, "The drone job market: What is it and where is it going?" *DroneLife*, 2019, [Online]. Available: https://dronelife.com/2019/02/07/droneii-the-drone-job-market-what-is-it-and-where-is-it-going/. [Accessed March 1, 2020].

[41] French-Post, "Trust your postman to look after your parents," [Online]. Available: www.laposte.fr/veiller-sur-mes-parents/les-visites-du-facteur-une-prevention-contre-l-isolement-des-personnes-agees. [Accessed March 1, 2020].

[42] A. Sousa-Poza and A. A. Sousa-Poza, "Well-being at work: a cross-national analysis of the levels and determinants of job satisfaction," *The journal of socio-economics*, vol. 29, no. 6, pp. 517–538, 2000.

[43] F. Schenkelberg, "How reliable does a delivery drone have to be?" in *2016 annual reliability and maintainability symposium (RAMS)*. IEEE, 2016, pp. 1–5.

[44] A. la Cour-Harbo, "Mass threshold for 'harmless' drones," *International Journal of Micro Air Vehicles*, vol. 9, no. 2, pp. 77–92, 2017.

[45] C. A. S. Authority, "Human injury model for small unmanned aircraft impacts," *Monash University: Melbourne, Australia*, 2013.

[46] A. Radi, "Potential damage assessment of a mid-air collision with a small uav," Civil Aviation Safety Authority, Monash University, Tech. Rep., 2013.

[47] J. A. for Rulemaking of Unmanned Systems, "Specific operations risk assessment," 2017, [Online]. Available: http://jarus-rpas.org/sites/jarus-rpas.org/files/jar_doc_06_jarus_sora_v1.0.pdf. [Accessed March 1, 2020].

[48] K. H. Terkildsen and K. Jensen, "Towards a tool for assessing uas compliance with the jarus sora guidelines," in *2019 International Conference on Unmanned Aircraft Systems (ICUAS)*. IEEE, 2019, pp. 460–466.

[49] K. Hartmann and K. Giles, "Uav exploitation: A new domain for cyber power," in *2016 8th International Conference on Cyber Conflict (CyCon)*. IEEE, 2016, pp. 205–221.

[50] T. Jones, "International commercial drone regulation and drone delivery services," RAND, Tech. Rep., 2017.

[51] N. Manders-Huits, "What values in design? the challenge of incorporating moral values into design," *Science and engineering ethics*, vol. 17, no. 2, pp. 271–287, 2011.

[52] M. A. da Silva Ferreira, G. C. Lopes, E. L. Colombini, and A. da Silva Simões, "A novel architecture for multipurpose reconfigurable unmanned aerial vehicle (uav): concept, design and prototype manufacturing," in *2018 Latin American Robotic Symposium, 2018 Brazilian Symposium on Robotics (SBR) and 2018 Workshop on Robotics in Education (WRE)*. IEEE, 2018, pp. 443–450.

[53] D. J. Bier and M. Feeney, *Drones on the Border: Efficacy and Privacy Implications*. Cato Institute, 2018.

[54] P. Boucher, "'you wouldn't have your granny using them': drawing boundaries between acceptable and unacceptable applications of civil drones," *Science and engineering ethics*, vol. 22, no. 5, pp. 1391–1418, 2016.

[55] J. Straub, "Unmanned aerial systems: Consideration of the use of force for law enforcement applications," *Technology in Society*, vol. 39, pp. 100–109, 2014.

[56] T. Stock and G. Seliger, "Opportunities of sustainable manufacturing in industry 4.0," *Procedia Cirp*, vol. 40, pp. 536–541, 2016.

[57] S. Spiekermann, *Ethical IT innovation: A value-based system design approach*. Auerbach Publications, 2015.

[58] IEEE, "Ieee p7000 - engineering methodologies for ethical life-cycle concerns working group," [Online]. Available: https://sagroups.ieee.org/7000. [Accessed March 1, 2020].

[59] ——, "The ethics certification program for autonomous and intelligent systems," [Online]. Available: https://standards.ieee.org/industry-connections/ecpais.html. [Accessed March 1, 2020].

[60] Danish-Municipalities, "Her ligger dit supersygehus - here is where your superhospital is located," 2015, [Online]. Available: http://www.danskekommuner.dk/Global/Artikelbilleder/2015/DK-3/DK-3-side-26-27.pdf. [Accessed March 1, 2020].

[61] HealthDrone, "Healthdrone website," 2019, [Online]. Available: https://sundhedsdroner.dk/index.php?page=the-project. [Accessed March 1, 2020].

[62] Danish-Traffic-Authority, "Order on flights with drones in built-up areas," 2017, [Online]. Available: https://www.trafikstyrelsen.dk/da/-/media/TBST-EN/Civil-aviation/Order-on-flights-with-drones-in-built-up-areas.pdf. [Accessed March 1, 2020].

[63] UN, "Un3373 biological category b for infectious or potentially infectious substances," [Online]. Available: https://www.un3373.com/category-biological-substances/category-b. [Accessed March 1, 2020].