2014 International Conference on Unmanned Aircraft Systems (ICUAS)
May 27-30, 2014. Orlando, FL, USA

Architecture Requirements for Ethical, Accurate, and Resilient Unmanned Aerial Personal Remote Sensing

Calvin Coopmans
AggieAir Group
Utah Water Research Laboratory and
Department of Electrical and Computer Engineering
Utah State University
Logan, Utah 84322
Email: c.r.coopmans@ieee.org

***Abstract*—It is undisputed that number of Unmanned Aerial Systems (UASs) will increase in the coming years. Small unmanned aerial scientific remote sensing systems or "data drones" have great potential to assist the human race with difficult problems such as water management and biofuel production, provided these systems can be integrated properly into society and airspace. The US Federal Aviation Administration (FAA) ideally will present rules for integrating UASs into National Aerospace System (NAS) by 2015. Ethics, safety, and data quality are the fundamental architectural components required for successful operation of autonomous aerial remote sensing systems, enabling integration into society and ultimately providing the benefits of these emerging technologies. In aviation, safety is the primary concern. In case of UAS and Personal Remote Sensing (PRS), the sole purpose of flight is to collect data; thus data is the Mission (i.e., the sole reason for airspace usage). Ethical principles for collection of information and personal privacy must also be included, to justify the use of UASs in civil (public) airspace while upholding the rights expected by civilians. Policies, standards, and agreements on architecture are necessary for producing systems which adhere to these fundamentals; aerial systems must include these basic properties in their designs to allow for lasting harmony between society and unmanned systems. In this paper, it is shown that any architecture which accomplishes this integration task must be compliant with the Architecture for Ethical Remote Information Sensing (AERIS) requirements. Several existing consumer-grade SUASs are evaluated based on these criteria and suggestions for AERIS compliance are given.**

I. Introduction

As Unmanned Aerial Systems grow in functionality and utility and mature in safety, applications for these versatile platforms will rapidly become abundant in the coming years. Civilian applications for UASs are an emerging field–one that has great potential and the possibility of explosive growth as their places in science and industry become secured. The US Congress is aware of these possibilities and has given the Federal Aviation Administration (FAA) a deadline of 2015 for the creation of rules allowing the inclusion and integration of UASs into the greater US National Airspace System (NAS), although integration and commercial use will likely be within 10 years of this date. This integration can not be determined by policy alone; the challenges and opportunities of addressing ethics and the public perception of UASs ([1]) will forever be a part of aviation and robotics as levels of integration and technology progress. It is hoped that the FAA's UAS access rules for the NAS will eventually be in the familiar form of 'file-and-fly,' and domestic UAS operations will be commonplace. With the proper certifications and standards, government and commercial operations will include regular UAS use, including integration into large-scale operations such as cyber-physical systems (CPS). As remote sensing is commoditized by smaller, more integrated systems, it will become practical at a personal level, represented by the term "Personal Remote Sensing" or PRS.

In this paper, first introduced are the scope and concepts of cyber-physical control (sec. I-A), ethical concepts (sec. I-B), interactions between architecture and policy (sec. I-C), and data mission success (sec. I-D). Then sec. II shows the three elements of PRS data mission success, and in sec. III, several existing UAS architectures are compared against the ideal for functionality and long-term cyber-physical potential. Finally, the paper concludes with final remarks and future work.

A. Cyber-Physical Control

Control and management of the real world are challenging, complex tasks. Processes interact at many spatial and temporal scales, but when engineered properly can be controlled just as a simple traditional process. With appropriate choices of sensors and actuators, closed-loop control can be implemented around any process, limited only by the desired outcomes of the controlled system and the complexity of the controller.

A cyber-physical controller (fig. 1) is a general structure that includes a real-world process (the "plant" in controls terminology), estimations of the dynamics of a process under control (an "observer"), and a controller. This allows closed-loop feedback to be instantiated for control of processes that might be outside traditional definitions of control, such as

978-1-4799-2376-2/14/$31.00 ©2014 IEEE

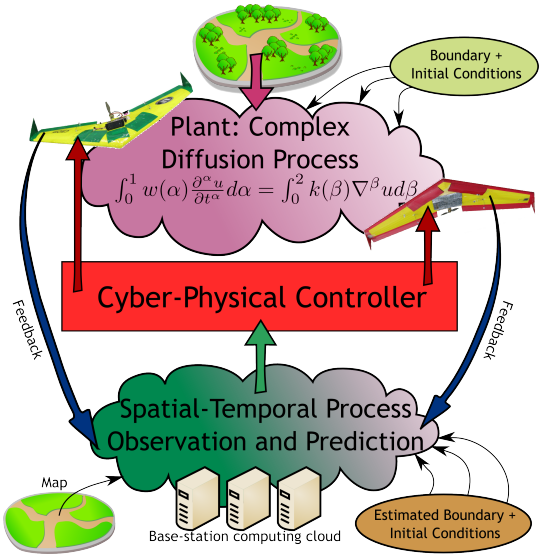


Fig. 1. The big picture of closed-loop cyber-physical system control

the moisture in a farm field, or the population of fish at an important aquatic site.

Models of physical processes can be used to help predict the behavior of a system in a particular scenario, or the reaction of a process to a given input. Cyber-physical control is enabled by modeling (usually digitally) a target process and utilizing that model to make decisions and exert control over the process by way of an actuator or a set of actuators. Since cognitive computer modeling and control of complex processes requires higher computational resources for higher accuracy, a computational cloud may be employed, distributing modeling tasks spatially and increasing reliability. Using advanced techniques such as fractional calculus [2], sophisticated models of physical processes can be constructed with proper boundary conditions, and when refined by quality data can reliably and robustly controlled in real time.

Control loops cannot be closed without feedback data. Due to the nature of cyber-physical control, the process under control can be multivariate, and therefore Cyber-Physical Controllers (CPCs) potentially have very broad requirements for sensing. Since in any closed-loop system better sensing equates to better control, providing CPCs with the most useful, or "best," data is of primary importance. This is one requirement UASs can effectively fulfill in CPSs: they can generate data with high spatial and temporal resolution about complex processes, allowing for CPC loops to operate on new and heretofore uncontrollable plants.

B. Ethics as Moral Behavior: Robots vs. Weapons

The study of ethics is a broad concept. However, unmanned ethics is becoming a pertinent topic and is absolutely critical to the operational success of civil RS UASs due to the significant ethical considerations of the operating environment and in the management of a RS UAS. Civil UAS missions can be defined as robotic tasks.

David Wright, a managing partner in Trilateral Research and Consulting [3] proposes a Privacy Impact Assessment (PIA) and give these unassailable ethical principles which must be adhered to for any project that deals with information [4]:

1) Respect for Human Autonomy
2) Avoiding Harm
3) Beneficence
4) Justice

These compare favorably with Isaac Asimov's classic Laws of Robotics. Asimov's robots serve for the good of humanity:

1) A robot may not injure a human being or, through inaction, allow a human being to come to harm.
2) A robot must obey the orders given to it by human beings, except where such orders would conflict with the First Law.
3) A robot must protect its own existence as long as such protection does not conflict with the First or Second Laws.

Any unmanned system which violates the above principals or laws cannot be considered a robot. In most cases, if these omissions are by design, a unmanned system is now a weapon (or strategic asset), as in the case of military operations.

There have been some attempts to discuss the ethics of UASs, but they have been focused on military or law enforcement applications ([5], [6]. These applications have more apparent moral dilemmas, and are more commonly covered by literature. Remote sensing applications more closely follow computer ethics and the ethics of information technology.

Some these concerns parallel the ethics of a Google Street View vehicle collecting information as it navigates routes on each continent. During its mission, a PRS UAS may collect inadvertent information–but what information is too private? What information and operations may affect the human operators? What effects does this have on the operating environment and airspace management? Only scale of operations and applicable laws can ultimately determine the answers.

It is also unethical to remain in the airspace if the quality of the data being collected is below a predefined threshold, since the data mission will have failed in this case.

C. Architecture-Driven Policy as the Solution to Long-Term Integration

The architecture of the rules and standards which control the airspace will determine the behaviors of the aircraft as well as the operators therein. Therefore, the architecture is of critical importance to the functionality of unmanned systems for data collection in the civil airspace.

In this study, an attempt is made to enumerate the major features such an architecture will need to be successful. The Architecture for Ethical Remote Information Sensing (AERIS) is proposed to allow scientific data collection flights while adhering to standards reasonably expected by civilians (privacy, safety, etc.).

Proper segmentation of the layers in system architecture is of critical importance (as espoused by Prof. John Doyle [7]),

and much can be learned about robustness to complexity from systems occurring in nature. Lessons can also be learned from poor layer separation in systems not designed for robustness such as the aging email architecture [8], insecure computer operating systems such as Microsoft Windows 95, or conflict-of-interest situations such as bribery in government.

D. Successful Data Missions

Three main components are needed for successful PRS/CPS data missions flying in civil airspace:

Data as the mission: Unmanned aerial systems for personal remote sensing (PRS) are, like any unmanned system, defined by their missions. Personal remote sensing, however is focused on data collection, and therefore a PRS mission can be defined directly as data. While quality as a concept is notoriously difficult to define [9], Data Mission Quality (DMQ) is a measure of the relative quality of the data mission, and can be used as a yardstick to compare multiple missions, different UASs, and different payloads.

Mission assurance, in a PRS sense, is Data Mission Assurance (DMA). Data Mission Assurance is the upholding of a minimum DMQ. This means, for example, without a fully functional payload, there is little reason to fly and make use of the airspace allocated to the SUAS.

The concepts of layering and modularity must be extended to the context of the greater civil airspace and expressed in a cyber-physical systems context to enable PRS systems to interact with manned aircraft and other UASs while in operation in a safe and reliable way, while delivering DMQ overall.

Ethics: Remote sensing applications more closely follow computer ethics and the ethics of information technology and medical record handling, and deserve specific, detailed, and clear directions for accountability and transparency in remote data collection. In addition, RS data has been collected for years in manned aircraft, while privacy complaints have not been prominent.

Management of airspace safety: The U.S. Federal Aviation Administration (FAA) manages the civil airspace and sets standards for airworthiness in the U.S. An overall AERIS-compliant architecture is needed for the thousands of small UAS to interact, and fly safely. Therefore, thoughtful architectures and policies based on those architectures are needed.

II. The Three Elements of Ethical Aerial Scientific Data Collection

To accomplish the PRS and CPS goals, AERIS architecture has three main areas of definition. They are Airspace Management, Data Mission Success, and Privacy by Design.

A. Airspace Management for Safety

The FAA has defined the Safety Order of Precedence [10]. Seen in priority Table I, this order of precedence refers to how a safety management system should be designed. The most reliable safety systems have the highest priority, while the least reliable systems must be used sparingly as they are the highest risk to system safety. The safety order of precedence in Table I is the approach for all safety considerations that is needed to enforce safety through architecture. Airworthiness addresses the first two priority levels of safety by incorporating fail-safes, system redundancies, and automatic termination sequences. Any active part of the system not requiring human intervention is the first priority in designing safety.

TABLE I
Table of FAA Safety Priorities

Description	Priority
Design for minimum risk	1
Incorporate safety devices	2
Provide warning devices	3
Develop procedures and training	4

1) **Airworthiness Issues** automatic safety elimination, or hazard reductions
2) **Human Factor Issues** Incorporating human-automation interaction developments, such as heads-up displays to improve Situational Awareness
3) **Concept of Operations** Standardized procedures and operations
4) **Training, documentation**s Standardized systems ([11], Appendix B (Page 24) for example logging requirements)

When automatic safety systems are not capable, the burden of safety becomes placed on the human operator.

Situational awareness and the optimization of operator cognitive load will help ease human-UAS interaction. Training systems, documentations and certifications fall into the last level of safety. These are traditionally the least reliable methods for ensuring safety.

Dependability engineering, Airspace regulations: Loss of safety is always the end of mission. This can happen for a variety of reasons, in part:

1) Human factors failures
2) Airworthiness issues
3) Flight hours (wear) on components
4) A given airframe's safety history
5) Crew training hours and history
6) Failure of forward-looking cameras or other safety pilot hardware
7) Failure of automatic dependent surveillance-broadcast (ADSB [12]) or applicable future technologies

B. Data Mission Success ("Dataworthiness")

Since data is the mission during PRS, a UAS must be able to estimate the quality of the data during progress. Data mission quality estimation can then lead to data mission assurance, and eventually to mission success, and scientific data fidelity.

Technical aspects of instrumentation, UAS flight-specific factors

Data mission quality is of course directly effected by the quality of the data itself. Sensor quality, weather, and many other factors are at play when a PRS system is collecting data:

1) Airframe (data from autopilot and other autopilots in a swarm)
    a) Control efforts (detect actuator damage, etc.)
    b) Battery performance and quality
    c) Motor performance (engine efficiency and wear for combustion powered-aircraft)
    d) Flight hours on components
    e) Wind and other environmental effects
    f) Navigation performance (Kalman filter convergence, sensor noise estimates)
2) Payload (Data quality metrics)
    a) Voltage and current on power supply rails
    b) Vibration statistics
    c) Sensor-specific quality metrics, such as thermal camera core temperature drift, camera capture times, etc.
    d) Data mission completeness (from other UASs in the mission as well)

C. Ethics: Privacy by Design

Ethical considerations for data collection are the major political barriers for allowance of RS UASs into the civil airspace. The collection of data by RS systems could capture sensitive or private details and lead to a violation of the right to reasonable privacy (for those inadvertently "caught" by the data collection system). This lack of control and lack of accountability naturally leads to fear, and therefore to intolerance.

Personal remote sensing systems need to have good boundaries with data i.e., prevention of misuse, before (planning), during (flight path rules), and after (data security), as well as prevention of hacking or other unauthorized access overall. Privacy is an expected right [4], and therefore must be preserved.

The ethics surrounding using UAS RS systems to collect data is most closely related to computer ethics [13]. One approach to solving these problems is called "privacy by design," or PBD [14]. Privacy by design is an architecture-based solution to the privacy issue by engineering a data collection system to account for privacy from the ground up.

In part, PBD defines 7 rules for data sensing UAS missions (from [14], where the term 'drone' is used for UAS):

1) The purpose for which the drone will be used and the circumstances under which its use will be authorized and by whom
2) The specific kinds of information the drone will collect about individuals
3) The length of time for which the information will be retained
4) The possible impact on individuals' privacy
5) The specific steps the applicant will take to mitigate the impact on individuals privacy, including protections against unauthorized disclosure
6) The individual responsible for safe and appropriate use of the drone
7) An individual point of contact for citizen complaints

Since the PBD effort is comprehensive and has momentum, an AERIS-compatible architecture should abide by the most current PBD ruleset.

D. Existing UAS Architectural and Ethical Research

AERIS compliments existing SUAS architecture literature. Quality work has been done targeting the large-scale integration problems UASs in the NAS will experience, but mainly from a communications and control perspective [15], and more encompassing work such as [16]. Cyber-physical perspectives on crop management and actuation are also being investigated [17], but without inclusion of ethical or safety concerns. Other literature focuses on ethical ramifications of UAS data collection (in the case, video and spy-style flight) [18] or cloud-enabled civil applications [19], without the inclusion of an overall architectural viewpoint. A broader view of safety is taken in publications such as [20] and [21], but no treatment of scientific data collection or CPS is included.

III. An Analysis of Open Source Robotic and UAS Architectures and Comparison to AERIS

AERIS compliance is challenging for current UASs, mainly because it involves more than simple engineering and technical solutions. Nevertheless, several excising architectures for robotic missions are analyzed in this section, to determine their ability for AERIS compliance or lack thereof. Since AERIS is all-encompassing and is based in many different aspects of UAS design, implementation and operation, the following systems are evaluated by their contributions to AERIS compliance if not their fulfillment.

A. Safety and Airworthiness

Aerospace applications are high-risk, engineering and testing standards are commonplace. To be testable and verifiable is the ultimate goal of aerospace system design, so risks are categorized and quantifiable. To this end, testability is very important for ethical use of airspace, and higher engineering standards can use used to provide lower risk levels and better AERIS compliance.

1) Airspace Management: The best way to measure how a UAS fulfills the airspace management segment of an AERIS-compliant architecture is the FAA's Safety Order of Precedence [10]. The highest priority is designing for minimum risk. A UAS can fulfill this by using a clearly written source code which is well tested. From a hardware point of view it is important to know the maximal drift of the navigation system–Inertial Measurement Unit (IMU) and Attitude and Heading Reference System (AHRS). Usually these values are provided in deg/hour; the magnitude of drift limits the GPS-denied mission time (beyond which the estimated attitude can be too far beyond a safe level of variance to be considered safe).

Fail-safe devices are implemented as a state-space machine covering possible situations with emergency flight termination

TABLE II
TABLE UAS BEHAVIORS WHICH ARE SIMPLE AND USEFUL

Loss of telemetry link – return to the base
Loss of radio link – emergency landing or return to the base
Loss of GPS – emergency landing
Low battery – return to the base

procedures. For example, UAS behaviors which are simple and useful:

Warning devices (priority 3) are provided to the Ground Control Station operator, who sees the airframe telemetry. However, during complicated missions when the cognitive load is too large, a simple visualization of data is not sufficient. To get the operator and pilot's attention, additional devices have to be implemented - for example audio and visual warnings. Since many UASs do not implement these features, they must be added to be AERIS compliant.

Safety procedures for the crew are important part of the overall airworthiness, but most UASs do not provide specific instructions.

2) Dataworthiness: Currently most UASs are developed as an autopilot and a ground control station only. In the autopilot code, they can provide data about the airframe (navigation, control efforts, battery monitoring etc.), however the payload data (Data Quality Metrics) are not part of most UASs and are not included with their standard mission code.

3) Ethics: Privacy By Design: Ethical constraints are the most difficult to implement. Most UASs are not designed for privacy from inception. Currently the responsibility for ethical use of the UAS with most systems depends solely on the operational crew. Although some ethical measures are commonly implemented (such as a predefined flight plan), much work still must to be done in this field.

B. RT-Paparazzi

Paparazzi is a free and open-source hardware and software project intended to create an exceptionally powerful and versatile autopilot system for fixedwing aircrafts as well as multicopters by allowing and encouraging input from the community [22]. Paparazzi is released under the GNU [23] license. A real-time port of the Paparazzi autopilot code, RT-Paparazzi, was shown in 2013, and this for this study, it is considered from a features and functionality standpoint.

RT-Paparazzi has two main parts, the Airframe segment (containing code for avionics and additional sensors) and the Ground segment (Ground Control Station interface, compiler tool-chain and some additional tools). The Airframe segment is based on ChibiOS [24] and written in C (for embedded hardware), the Ground segment in OCAML [25] and Python with some specific tools in MATLAB.

The overall Paparazzi structure is pictured in fig. 2, and is a generalized version of the command and control loop of a flying UAV. This system is controlled by a ground station, which commands the UAV to fly from waypoint to waypoint, however the actual control law remains as in fig. 2.

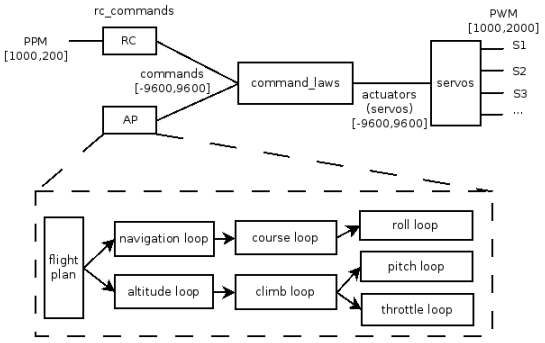


Fig. 2. An overview of the Paparazzi control scheme from [22]

Safety and Airworthiness: Since RT-Paparazzi is implemented in a real-time OS, it is possible to measure timing and verify each thread's performance both on the ground during testing and in flight. Software upsets can be detected in flight to detect errant code or hardware, but these mitigation decisions are left up to the operators during the UAS mission.

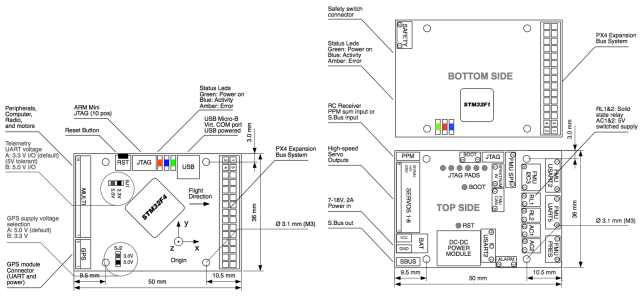
Airspace Management: Paparazzi implements all of the behaviors in Table II

Dataworthiness: Paparazzi alone does not implement remote sensing payload functionality directly. However, due to the open-source nature of the project different payload interfaces are possible though defined I/O on the autopilot board.

Ethics: Privacy By Design: Ethical constraints are the most difficult to implement for any UAS. Paparazzi is not an exception; it was not designed for privacy from inception. Currently the responsibility for ethical use of the UAS with Paparazzi system depends solely on the crew.

C. PixHawk PX4

The Pixhawk autopilot system is a project of many contributors, managed by ETH Zurich [26]. Like Paparazzi, Pixhawk's PX4 autopilot (diagramed in fig. 3 is not a true UAS, however 3D-Robotics [27] sells fully integrated and tested rotary-wing unmanned platforms based on the PX4.



(a) The Pixhawk PX4 FMU [26] (b) The Pixhawk PX4 IO board [26]

Fig. 3. An overview of the PixHawk avionics system from [26]

Safety and Airworthiness: The Pixhawk PX4 autopilot system is comprised of two major parts (both seen in fig. 3): the Flight Management Unit (FMU) and an I/O module with

TABLE III
TABLE OF UAS AND AUTOPILOTS STUDIED FOR PERSONAL REMOTE SENSING VIABILITY

UAS Name	Inception	(Hardware) Platforms	Cost	CPU(s)	Nav. Sensor Suite	Sensor Options
(RT) Paparazzi	2003	(Multi) Fixed-wing, Rotary	$	168Mhz 32bit w/FPU	Many	Many
3D-Robotics Pixhawk (PX4)	2009	(Single) Fixed-wing, Rotary	$	168Mhz 32b w/FPU + 72Mhz 32b	Proprietary IMU	Many
Robot Operating System (ROS)	2007	(Linux-based) General	$	Dependant on CPU	None/Many	Many
DJI Phantom (2.0)	2011	(Proprietary) Rotary	$$	Not published	Proprietary IMU	Few
AggieAir (2.0)	2007	(Multiple) Fixed-wing, Rotary	$$$	168Mhz 32bit w/FPU + 1200 MIPS Linux	3DM GX3/Many	Many

UAS Name	Control BW (Hz)	Ext. Airborne Interfaces	Payload for Remote Sensing?	AERIS Compliance Possible?
(RT) Paparazzi	500	I2C, SPI, CAN-Bus, Serial, A/D	No	Not as implemented
3D-Robotics Pixhawk (PX4)	200	I2C, SPI, CAN-Bus, Serial, A/D	No, Possible	Not as implemented
Robot Operating System (ROS)	Dependant on CPU	Any Linux	No, Possible	Not as implemented
DJI Phantom 2 Vision	200	Micro USB, CAN-Bus	No, Inc. Gimble Camera	Not as implemented
AggieAir (2.0)	500	I2C, SPI, CAN-Bus, Serial, A/D, Ethernet	Yes	Yes

power, interfacing, and a backup/override processor to allow for redundant manual flight control should the main autopilot encounter and error condition. Like RT-paparazzi, the PX4 autopilot system is implemented in a real-time operating system (NuttX [28]) and therefore is expandable and testable for software errors before and during flight.

Airspace Management: The Pixhawk system implements all of the behaviors in List II, depending on its configuration.

Dataworthiness: The Pixhawk system alone does not implement remote sensing payload functionality directly, although throughout its history image capture and processing as been targeted as a mission parameter. Due to the open-source nature of the project different payload interfaces are possible though defined I/O on the avionics system boards. In addition, at the time of this writing, the Pixhawk project reports upcoming integration with ROS (see sec. III-D) for a more integrated robotic system, which could give the Pixhawk system enough computational oversight to comply with AERIS.

Ethics: Privacy By Design: As with most of the listed UASs, ethical constraints are not implemented in a technical sense and depend solely on the crew. Since the PX4 system can fly fixed-wing and rotary-wing craft, which pre-programmed waypoint flight it is possible to avoid untended data gathering during mission planning.

D. ROS

One example of a successful robotic architecture is the Robot Operating System, ROS [29] is flexible and extensible, and implements the main aspects of Doyle's architecture requirements (data and process separation). ROS is node-based, allowing designers to implement data and behavior flows as they deem necessary at a high, graph-based level. The operating system is in the middle of the bow-tie, coordinating data and action in a robust way.

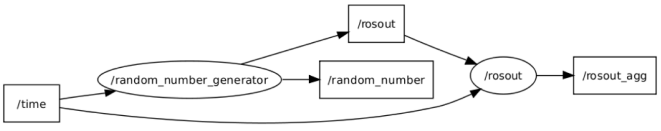


Fig. 4. The node-based architecture of ROS, from [29]

Safety and Airworthiness: ROS is based on solid design principals, but does not target high-speed hard real-time processing. Since ROS is implemented as software running on a Linux kernel, ROS is missing the critical element of real-time feedback and control to operate a UAS safely.

Airspace Management: Since ROS is not specifically targeting UAS use, it is not specifically oriented to airspace management. However, it is possible to implement all of the behaviors in Table II.

Dataworthiness: ROS is superior to many UASs with respect to dataworthiness, since it is designed to provide reliable software/hardware interfaces to sensors such as 3D cameras, GPS, etc. However, without pairing with a true autopilot system such as Paparazzi or Pixhawk, ROS is not a good candidate for a full AERIS-compliant UAS.

Ethics: Privacy By Design: Ethical constraints are not implemented in a technical sense within ROS, but due to ROS's high-level functionality it is more possible to implement computational oversight such as no-fly boundaries, etc. As stated above, ROS must be paired with a true UAS autopilot system, as well as an ethical support network to fulfill AERIS requirements.

E. DJI Phantom 2 Vision

Developed by Da-Jiang Innovations Science and Technology Co., Ltd. of Shenzhen, China, the DJI Phantom 2 Vision UAS [30] is a full flight system (unmanned aircraft, safety pilot control system) with gimbaled HD camera pictured in fig. 5. Complete with a 14mp camera, when coupled with an iOS or Android mobile device as a ground station, the DJI Phantom allows for pre-planed flight maneuvers (i.e., beyond line-of-sight), and 1080p HD video or still pictures to captured and transmitted down to the operator. Easy social sharing features (Facebook, Twitter, etc.) allow for instant propagation of media captured when the ground station device (iPhone, etc.) has an Internet connection. The low cost of entry and ease of use of the Phantom 2 make UAS technology truly more available than before.

Safety and Airworthiness: Although DJI has been making autonomous rotary hardware for hobbyist/enthusiast market for many years, the Phantom 2 Vision represents the first mass-market full image and video platform with GPS way-

Fig. 5. The DJI Phantom 2.0 Rotary UAS from [30]

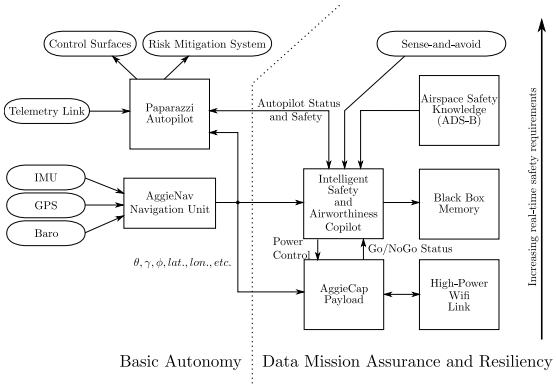


Fig. 6. AggieAir Block Digram with ISaAC

point and other autonomous pre-programmed functionality. Although DJI does not make full system specifications open to users or developers, interfaces like CAN bus show a outward commitment to airworthiness.

Airspace Management: While the Phantom 2 Vision does implement the behaviors in Table II, it is intended solely for noncommercial use in the U.S. However high-quality camera options (such as the now film industry-standard GoPro) show the obvious (and subtly marketed) possibilities for commercial video and still image collection e.g. movie/commercial camerawork or realtor house imagery. Since these applications are forbidden by the FAA, there is no way to manage them safely in the airspace.

Dataworthiness: Although camera options such as gimbals and GoPro sensors are attractive for its target market, they have little to no value in the AERIS-style of remote sensing. No information about the quality of the data recorded by the camera is stored. For AERIS-compliant missions, the Phantom 2 is at a low level of dataworthiness for PRS CPS work.

Ethics: Privacy By Design: Since ethics have not been considered in the DJI design, and since the Phantom 2 and other DJI and DJI-style autonomous aircraft are mass produced and are more capable and accessible than before, it is likely that the mass production of this kind of craft actually represents a net lowering of the ethical qualifications. Crew training, ethical training, no-fly considerations are not given with the DJI system and are therefore left to the consumer users of the hardware.

F. AggieAir 2.0

Originating at CSOIS [31] in 2006, the AggieAir 2.0 UAS (previously published: [32], [33], [34]) uses a modified Paparazzi autopilot and environment for PRS missions in various environments and missions. Paparazzi, evaluated separately in sec. III-B, controls all AggieAir UASs, and is shown in fig. 2. The AggieAir UAS flight system diagram is seen in fig. 6, which includes the ISAaC safety co-pilot detailed in previous publications [35].

Safety and Airworthiness: AggieAir has many hours over several years of autonomous flight by way of the Paparazzi UAS. With the advent of the RT-Paparazzi branch, much like the Pixhawk system, hard real-time processing targets can be made and verified, allowing for better testing before flight, and more knowledge of software inconsistencies during flight. Mitigation strategies such as emergency landing or mission termination via parachute can be deployed depending on the failure analysis

Airspace Management: In addition to the behaviors in Table II, AggieAir flies under a COA with a PIC (pilot in charge) to interface with the local airspace and avoid collision conditions. Coupled with comprehensive training, this allows AggieAir to fly safely and manage airspace.

Dataworthiness:

To achieve DMA in current AggieAir payloads, modular approaches to PRS UAS systems design are taken, from development to testing, allowing overall performance and system faults to be quickly and accurately diagnosed. AggieAir has augmented Paparazzi with a modular payload architecture which embodies AERIS-compliant payload design [35], also seen integrated in the AggieAir UAS in fig. 6, this design has captured remote sensed data successfully over many hours of safe, autonomous flight (for example, thermal infrared data collection [36]). This is a higher-level approach, which brings Paparazzi to a layered PRS based on DMQ (along the lines of Doyle and larger Aerospace design).

Ethics: Privacy By Design: Because the Paparazzi UAS only provides a base for the AggieAir operations, ethical concerns are handled at the crew level. This means that AggieAir's standard mission practice is to keep a high-level of security around collected data, as well as only flying missions around targeted agricultural and natural resource areas, avoiding populated and otherwise sensitive subjects. Also, data containing personally identifiable content is deleted, assuring the privacy of any private subjects who might be unwittingly imaged. This makes AggieAir the most AERIS compliant of all the UASs profiled.

G. AERIS in current UASs

Overall, many current UASs provide solid bases for AERIS-compliant architecture, but additional systems still have to be implemented to fully comply with the requirements. Current UASs like Paparazzi were not originally developed with AERIS-stye requirements, and therefore the next generation of UAS architectures must be AERIS-compliant at the design stage due to the impracticality of retrofitting older designs.

IV. Conclusion

The future of UASs is undoubtedly bright. While the current public perception of UASs is one of espionage and warfare, they will become more accepted into domestic use as their potential value becomes apparent and as the airspace rules change to include them. While current regulations of UASs are restrictive and limited in the US, soon UASs will become available for regular use as standards for certification and airworthiness are developed.

Along with these standards, mission quality metrics are needed to determine if the UAS is truly in need of the airspace. Along with ethics (privacy by design), am AERIS-compliant airspace access requirement architecture will allow civil flights of many kinds with minimal concern for right violations, allowing humans and unmanned robotic systems to peacefully coexist and grow together.

Future work for this topic is in all presented avenues of policy, engineering to create workable architectures (both inside and outside UASs) that protect rights, uphold safety, and better the world for both man and machine.

Acknowledgment

The author would like to thank Dr. Mac McKee and Austin Jensen of the AggieAir flying circus, Dr. YangQuan Chen and Brandon Stark of the U.C. Merced MESA lab, as well as the large Paparazzi open-source community.

This project is supported in part by Utah Water Research Laboratory MLF 2006-2014 and by the NASA UAS2NAS program (Grant # NNX11AO77A).

References

[1] P. Oh, "Forward," in *Remote Sens. Actuation Using Unmanned Veh.* Hoboken, New Jersey: John Wiley & Sons, 2012, pp. xxi—-xxii.

[2] Z. Jiao, Y. Chen, and I. Podlubny, "Introduction," in *Distrib. Dyn. Syst.* Springer London, 2012, pp. 1–10.

[3] D. Wright and M. Partner, "An integrated privacy and ethical impact assessment Definition of PIA," 2012.

[4] D. Wright, "A framework for the ethical impact assessment of information technology," *Ethics Inf. Technol.*, pp. 199–226, 2011.

[5] R. C. Arkin, "Governing Lethal Behavior: Embedding Ethics in a Hybrid Deliberative/Reactive Robot Architecture PART I: Motivation and Philosophy," in *Proc. 2008 3rd ACM/IEEE Int. Conf. Human-Robot Interact.*, 2008, pp. 121–128.

[6] R. L. Finn and D. Wright, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications," *Comput. Law Secur. Rev.*, vol. 28, no. 2, pp. 184–194, 2012.

[7] J. Doyle, "Universal laws and architectures," *CDS 212 Lect. Notes*, 2011. [Online]. Available: http://www.cds.caltech.edu/~doyle/wiki/images/1/16/2_DoyleSageLec2_May14_2012.pdf

[8] M. Ferris and U. Treasury, "New email security infrastructure," in *New Secur. Paradig. Work.*, 1994, pp. 20–27.

[9] S. Consigny, "Rhetoric and madness: Robert Pirsig's inquiry into values," *South. Speech Commun. J.*, vol. 43, no. 1, pp. 16–32, Dec. 1977.

[10] Federal Aviation Administration, "System Safety Handbook," 2000.

[11] US Federal Aviation Administration, "Unmanned Aircraft Systems Test Site," 2013.

[12] C. P. Lai, Y. J. Ren, and C. Lin, "ADS-B based collision avoidance radar for unmanned aerial vehicles," in *Proc IEEE MTT-S Int. Microw. Symp. Dig. 2009. MTT'09.*, 2009, pp. 85–88.

[13] D. G. Johnson, *Computer ethics*. DIANE Publishing Company, Dec. 1998, vol. 30, no. 4.

[14] A. Cavoukian, "Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices," *Inf. Priv. Comm. Ontario, Canada*, 2009.

[15] P. P. Narayan, P. P. Wu, D. A. Campbell, and R. A. Walker, "An Intelligent Control Architecture for Unmanned Aerial Systems (UAS) in the National Airspace System (NAS)," May 2007.

[16] C. W. Heisey, A. G. Hendrickson, B. J. Chludzinski, R. E. Cole, M. Ford, L. Herbek, M. Ljungberg, Z. Magdum, D. Marquis, A. Mezhirov, J. L. Pennell, T. A. Roe, and A. J. Weinert, "A Reference Software Architecture to Support Unmanned Aircraft Integration in the National Airspace System," *J. Intell. Robot. Syst.*, vol. 69, no. 1-4, pp. 41–55, Aug. 2012.

[17] B. S. Faiçal, F. G. Costa, G. Pessin, J. Ueyama, H. Freitas, A. Colombo, P. H. Fini, L. Villas, F. S. Osório, P. A. Vargas, and T. Braun, "The use of unmanned aerial vehicles and wireless sensor networks for spraying pesticides," *J. Syst. Archit.*, vol. 60, no. 4, pp. 393–404, Apr. 2014.

[18] R. L. Finn and D. Wright, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications," *Comput. Law Secur. Rev.*, vol. 28, no. 2, pp. 184–194, Apr. 2012.

[19] U. Pagallo, "Robots in the cloud with privacy: A new threat to data protection?" *Comput. Law Secur. Rev.*, vol. 29, no. 5, pp. 501–508, Oct. 2013.

[20] P. Lin, K. Abney, and G. Bekey, "Robot ethics: Mapping the issues for a mechanized world," *Artif. Intell.*, vol. 175, no. 5-6, pp. 942–949, Apr. 2011.

[21] R. Clarke, "What drones inherit from their ancestors," *Comput. Law Secur. Rev.*, vol. 30, no. 3, pp. 247–262, Jun. 2014.

[22] Paparazzi Forum, "Open Source Paparazzi UAV Project," 2008. [Online]. Available: http://paparazzi.enac.fr/

[23] "GNU, General Public License, full description." [Online]. Available: https://www.gnu.org/licenses/gpl.html

[24] "ChibiOS/RT." [Online]. Available: http://www.chibios.org/

[25] "OCaml, the Objective Caml." [Online]. Available: http://ocaml.org/

[26] "Pixhawk project homepage." [Online]. Available: http://pixhawk.org/

[27] "3DRobotics Homepage." [Online]. Available: http://3drobotics.com/

[28] "NuttX Real-Time Operating System." [Online]. Available: http://nuttx.org/

[29] "ROS (Robot Operating System)," 2011. [Online]. Available: http://www.willowgarage.com/

[30] "DJI Phantom 2 Product Homepage." [Online]. Available: http://www.dji.com/product/phantom-2/

[31] "Center for Self-Organizing and Intelligent Systems." [Online]. Available: http://www.csois.usu.edu/

[32] "AggieAir Flying Circus." [Online]. Available: http://aggieair.usu.edu/

[33] C. Coopmans, L. Di, A. M. Jensen, A. A. Dennis, and Y. Chen, "Improved Architecture Designs for a Low Cost Personal Remote Sensing Platform: Flight Control and Safety," in *ASME/IEEE Int. Conf. Mechatron. Embed. Syst. Appl.*, Sep. 2011, pp. 937–943.

[34] C. Coopmans and Y. Han, "AggieAir: An integrated and effective small multi-UAV command, control and data collection architecture," in *Proc. ASME IDETC/CIE 2009, 1st Small Unmanned Aer. Veh. Technol. Appl. (SUAVTA), 2009 ASME/IEEE Int. Conf. Mechatron. Embed. Syst. Appl.*, San Diego, California, USA, 2009, pp. 1–7.

[35] C. Coopmans, B. Stark, and C. M. Coffin, "A payload verification and management framework for small UAV-based personal remote sensing systems," in *Proc. 2012 Int. Symp. Resilient Control Syst.* IEEE, Aug. 2012, pp. 184–189.

[36] A. M. Jensen, B. T. Neilson, M. McKee, and Y. Q. Chen, "Thermal Remote Sensing With an Autonomous Unmanned Aerial Remote Sensing Platform for Surface Stream Temperatures," in *Proc. Int. Geosci. Remote Sens. Symp.*, 2012, pp. 5049–5052.