Ethical Concerns of Unmanned and Autonomous Systems in Engineering Programs

Prof. Richard S. Stansbury, Embry-Riddle Aeronautical Univ., Daytona Beach

Dr. Richard S. Stansbury is an associate professor of computer engineering and computer science at Embry-Riddle Aeronautical University in Daytona Beach, FL. His research interests include unmanned aircraft systems, field robotics, and applied artificial intelligence. He is program coordinator for ERAU's new MS in Unmanned and Autonomous Systems Engineering program, which began in fall 2013.

Mr. Joshua Lloyd Olds, Embry-Riddle Aeronautical Univ., Daytona Beach
Dr. Eric Joe Coyle, Embry-Riddle Aeronautical University

Eric J. Coyle received a B.S. in Mechanical Engineering from Clemson University and Ph.D. in Mechanical Engineering from Florida State University with a concentration in Dynamics and Controls. He was a postdoctoral fellow at the Center for Intelligent Systems, Control and Robotics (CISCOR) before joining Embry-Riddle Aeronautical University as an Assistant Professor of Mechanical Engineering in 2011. His research interests include robotics, computer vision, machine learning, rehabilitation engineering and controls.

Ethical Concerns of Unmanned and Autonomous Systems in Engineering Programs

Abstract:

Unmanned systems are entering educational curricula (both K–12 and post-secondary) because they capture student interest, provide multidisciplinary engineering opportunities, and demonstrate many tangible science, technology, engineering, and mathematics (STEM) concepts. In collegiate engineering programs, unmanned systems are used both within the curriculum (e.g. capstone design projects) and as part of co-curricular/extra-curricular activities (e.g. the Associate for Unmanned Vehicle Systems International (AUVSI)'s student design competitions). Graduate programs dedicated to unmanned systems engineering are beginning to emerge to provide specialized engineering skills to support an emerging industry. This paper seeks to investigate and report the various ethical issues that exist and must be considered with respect to engineering education involving unmanned and robotic systems.

This paper provides an overview of a new graduate program in unmanned and autonomous systems engineering, and addresses three major ethical issues to be addressed for such a program. For the first issue, the paper discusses current ethical debates such as privacy, public safety, liability, lethal use, etc., which ought to be consider during curricular and research activities involving unmanned systems. The second issue discussed involves how the engineering of unmanned systems relates to current professional codes of ethics from a number of relevant professional engineering societies, and how they are addressed currently within the program's curriculum. Finally, the paper addresses concerns regarding how and with whom technical information regarding the design and operation of unmanned systems can be safely, responsibly, and legally disseminated within the curriculum and university sponsored programs.

1.0 Introduction

The term "unmanned system" can refer to types of systems that were traditionally controlled either directly or indirectly through a human operator, but have through modern technologies been automated to no longer require a human operator. Examples of unmanned systems include: unmanned aircraft systems (UAS), unmanned surface vehicles (USV), unmanned ground vehicles (UGV), and unmanned underwater vehicle (UUV).

The study of unmanned systems emerging within educational curricula (both K–12 and post-secondary) because these systems capture student interest, provide multidisciplinary engineering opportunities, and demonstrate many STEM concepts. In collegiate engineering programs, unmanned systems are used both within the curriculum (e.g. capstone design projects) and as part of co-curricular/extra curricular projects (e.g. the AUVSI's Student Unmanned Aerial Systems Competition). Graduate programs dedicated to unmanned and autonomous systems engineering are now starting to be offered to provide specialized engineering skills to support an emerging industry.

This paper seeks to investigate and report the various ethical issues that exist that must be considered with respect to engineering education involving robotic systems. First, the paper

discusses educating students and student teams regarding the safe, legal, and ethical usage of experimental robotic systems such as UAS and autonomous automobiles. Second, the paper discusses how academic programs involving unmanned systems must address how and to whom information regarding unmanned technologies within our curriculum and university sponsored programs is disseminated. Lastly, the paper discusses educating students and faculty about unmanned technology specific ethical debates that currently exist within our society such as privacy, public safety, liability, lethal use, etc.; and how to responding to external criticism from the media and public.

2.0 Background

Embry-Riddle Aeronautical University, a private university, with two residential campuses, a number of satellite locations worldwide, and online, has been actively involved in unmanned systems academics and research for nearly a decade including an undergraduate academic program in unmanned aircraft system operations. These activities are curricular, co-curricular, and extra-curricular.

The University's College of Aviation offers one of the few 4-year undergraduate programs within the United States (U.S.) to train unmanned aircraft pilots and operators, Bachelor of Science in Unmanned Aircraft System Sciences. Students within its program are exposed to a number of aviation and engineering topics within their four-year degree program. Students are given the opportunity to reinforce their learning with co-curricular opportunities such as internships and hands-on projects, and extra curricular activities including participation within the AUVSI student unmanned systems competitions. In addition to a four-year baccalaureate degree, a minor in UAS is also available.

Within the College of Engineering, faculty performing teaching and researching within three major departments, Mechanical Engineering (ME); Aerospace Engineering (AE); and Electrical, Computer, Software, and Systems Engineering (ECSSE), have been actively involved with unmanned systems teaching and research. Active areas of research include systems comprised within or supporting UAS, UGV, Driverless Cars, USV, and UUV including platforms, sensors, systems, and computing.

The Robotics Association supports student projects, undergraduate, and graduate research allowing the university to compete in all AUVSI Foundation student competitions including: Intelligent Ground Vehicle Competition, sUAS, Aerial Robotics Competition, RoboBoat, and RoboSub. This organization supports a number of campus outreach initiatives.

In Fall 2013, a new cross-disciplinary graduate engineering degree program was launched for a Master of Science in Unmanned and Autonomous Systems Engineering (MSUASE). The MSUASE program is housed under the College of Engineering, but outside of any one department. The lead author is the program coordinator, who chairs a coordination committee with representatives from a number of departments across the college.

The MSUASE program is a 30 credit graduate program that is based around 15 credit hours of core coursework and 15 credit tracks (thesis, capstone, and course-based). The thesis track

requires nine credits of thesis and six credits of additional coursework. The capstone track requires six credits of capstone design course (3 credits per semester) and nine credits of additional course work. Lastly, the course-based track allows students to take 15 credits of additional coursework to complete their degree. The course-based track was specifically provided to support international students who may be prohibited from participating on some projects due to the restrictions discussed in Section 5 of this paper. To date, there are six students enrolled within the program for the Spring 2014 term.

3.0 Ethical Concerns for Unmanned Systems

Prior to discussing this topic in terms of traditional engineering codes of ethics, it is important to look at some of the philosophical concerns regarding unmanned systems. This section captures several issues currently debated within the public or literature. The authors are purposely remaining neutral on their personal stance with these issues.

3.1 Issue #1: Unmanned Systems for Military Applications

The development and utilization of unmanned systems for military applications is currently a highly contested and debated issue. For professional engineers and engineering faculty, the major concern is performing research sponsored by defense organizations such as the U.S. Department of Defense or a defense subcontractor.

Robotics researcher, Ronald Arkin, has written a number of papers[1,2] and a book[3] in support of developing ethical principles into war-fighting unmanned systems. His career has supported projects from ordinance disposal to the lethal Defense Advanced Research Project Agency (DARPA) Unmanned Ground Combat Program, which can be equipped with weapons[1]. He has also lead an effort funded by the U.S. Army Research Office (ARO) to embedded ethical models and decision making into robotic systems such as those described above[2,3].

In Arkin's work with ARO, he has provided a significant survey into the theories of a "just war" as well as examined the laws of war and rules of engagement, which dictate what actions can be taken and how the warfighter should conduct themselves on the battlefield. In one paper[2], Arkin's case is made regarding the history of lethal unmanned systems in combat and a discussion of the ethics of war. With Arkin's work, the goal to develop an artificial conscience to govern the use of lethal force by the unmanned systems is justified by a couple of key arguments. First, Arkin contends based upon documented evidence that human warfighters under wartime conditions are susceptible to committing and/or tolerating illegal acts. Therefore, creating an unmanned system capable of following international law and rules-of-engagement could potentially mitigate wartime atrocities. Second, he states that these efforts will occur "with or without my participation"[1].

A number of papers from a variety of forums speak out against unmanned systems for lethal military applications. An article by Sparrow entitled "Just Say No to Drones"[4]makes a passionate plea to engineers and others within the robotics committee to not accept funding from the military to support their research agendas. In addition to pointing out his views on the potential evils of war, Sparrow discusses that unmanned systems replacing warfighters while

sparing the lives of a solder can lower the threshold for entry to war by making the political costs lower, which could result in more frequent or more brutal wars. The paper discusses the concerns of the military funding "strong" artificial intelligence efforts, which could bypass many of the ethical/moral safeguards that ought to be integrated into a thinking machine. Lastly, Sparrow cautions against justifying military funding for the sake of dual-use / spinoff opportunities arising form the research. The article also discusses a number of efforts of robot ethicists to create an ethical guide for roboticists and engineers including the Euron Roboethics Roadmap[5].

Sharkey, a robot-ethicist, provides further counter-arguments against lethal robotic systems, and in particular unmanned systems that are capable of autonomously operating their weapons without direct human authorization. His arguments can be summarized by the following ethical questions, which must be considered. First, how do you define a non-combatant? How do you sense this? Sharkey contends that technologies sufficiently capable of differentiating a combatant from a non-combatant exist today. Second, how do you add intelligence on when to use lethal force and when it is not applicable? Sharkey contends that an unmanned system with kill authority would not have the same human capability to differentiate situations in which lethal force is necessary versus situations in which it could be avoided.

In the end, this is a hotly debated topic. It does provide some important considerations that can be posed to students during discussion within courses on unmanned systems and their applications. Furthermore, it does pose some questions to the faculty, staff, and administrators of institutions undergoing unmanned systems research regarding whether or not to accept military/defense funding and under what terms.

3.2 Issue: Privacy and Unmanned System Surveillance

Over the past decade, a growing concern of civil liberties groups and others is the impact of unmanned systems, particularly UAS, on privacy. The law enforcement community has been a major advocate for the integration of UAS into the U.S. National Airspace System (NAS) for applications including aerial surveillance, disaster response, traffic monitoring, etc. The 2012 FAA Reauthorization Bill[6] provided explicit language in support of expedited integration of UAS into the NAS, and in March 2013 a memorandum of understanding was established between the FAA and Department of Justice to streamline the issuing of Certificates of Authorization for law enforcement[7].

The American Civil Liberties Union (ACLU) has written a report entitles "Protecting Privacy from Aerial Surveillance: Recommendation for Government Use of Drone Aircraft"[8]. Unmanned system sensing capabilities of unmanned aircraft discussed include the use of high-power zoom lenses, thermal engineering, intelligent sensing (facial recognition, behavior profiling, etc.), synthetic aperture radar, etc. One major concern stated by the ACLU is mission creep in which unmanned aircraft approved for activities such as warranted surveillance or tactical overwatch could be later redeployed for activities such as monitoring the general public. They state the concern of utilizing UAS to track people and vehicle. Other concerns include the use for UAS transitioning from surveillance to intervention. Side effects of these concerns

include: continued state of concern over being watched, voyeurism, discriminatory targeting/profiling, etc.

AUVSI has weighted in on many of these concerns. The organization has contended that privacy issues such as those weighted in by the ACLU are not exclusive to unmanned aircraft, but are common to many modern surveillance technologies. They contend that existing Fourth Amendment protections as well as federal and state privacy laws provide sufficient protections to address the privacy concerns of the public[9].

Several guidance documents have been established that helps guide the industry. In July 2012, AUVSI released a Code of Conduct[10] to explicitly acknowledge the privacy concerns, among other concerns. The International Association of Chiefs of Police's Aviation Committee has produced the "Recommended Guidelines for the use of Unmanned Aircraft"[11], which provides explicit expectations for when UAS can be operated and how the data collected is stored/maintained. Finally, the FAA has weighted in on privacy concerns by mandating that FAA supported UAS test sites must provide a public privacy policy[12].

3.3 Other Issues

A number of additional ethics issues can be summarized as follows.

One concern closely tied to professional ethics is the attribution of responsibility associated with a mishap of an unmanned system. For instance, if a dock worker is injured on the job due to a failure of an unmanned system to detect and avoid that worker, would the liability be assessed to a human supervisor that is overseeing one or multiple unmanned systems at a time, the corporation owning and operating the docks, or would the liability fall onto the manufacturer for not providing adequate safeguards.

Another major concern, which Arkin states often provides more personal moral concern to himself than development of military robots is the impact that robots/unmanned systems have on employment[1]. For instance, if an unmanned forklift or crane takes the place of one or multiple dockworkers to produce an automated shipyard, is there a moral/ethical dilemma that exists. Arkin states that it can be seen as conflicting with two different personal philosophies, utilitarian, which would weigh in on benefit to industry, lowering of product costs, etc. vs. Kantian, which would draw issue with the workers' right to good will[1].

Cybersecurity concerns have also been raised. First, the ability of an unmanned system to be hacked could have serious consequences on the safety of the system and the perception of public safety. Second, the security and storage of the data collected by these systems is of concern as it could have additional consequences related to the privacy debate if compromised.

4. Professional and Ethical Responsibility

This section discusses the applicability of professional codes of ethics to the engineering of unmanned systems. This is relevant because it both guides the dialog/culture of an institution conducting such work, and, likewise, it must be communicated to the students. An

understanding of professional ethics is a necessary student outcome for both graduate and undergraduate engineering education programs.

4.1 Applying Professional Code of Ethics to Unmanned Systems

A common expectation of any engineering academic program is to produce graduates that can conduct themselves professionally and ethically within the workforce. Within the domain of unmanned systems, this must be addressed carefully to ensure that the expectations of a professional code of ethics are being addressed.

The Institute of Electrical and Electronics Engineers (IEEE) represents the professional society of Electrical Engineers, Computer Engineers, Software Engineers, and related professionals. For this paper, the IEEE Code of Ethics[13] shall be discussed such that the applicable terms of the code are addressed. Other relevant organizations such as American Society of Mechanical Engineers (ASME) and American Institute of Aeronautics and Astronautics (AIAA) also provide similar codes of ethics[14,15].

The first statement of the IEEE Code of Ethics reads that is members agree ``to accept responsibility in making decisions consistent with the safety, health, and welfare of the public, and to disclose promptly factors that might endanger the public or the environment"[13]. This statement is highly applicable to unmanned systems. First, the development of an unmanned vehicle such as an unmanned aircraft, driverless car, or autonomous sea vessel must be developed to ensure the safety of existing manned uses of their navigable operations spaces. Safe operation must be maintained during both nominal and off-nominal conditions (loss of data link, loss of GPS lock, etc.). Regulators such as the FAA have placed high standards for autonomous vehicles to provide an equivalent (or sufficient) level of safety. It is also of the utmost importance to articulate and report any mishaps or accidents that occur to determine that the public wellbeing is maintained and known risks are reported.

The third statement of the IEEE Code of ethics reads that its members agree ``to be honest and realistic in stating claims or estimates based on available [13]. Autonomous systems such as unmanned aircraft must undergo a certification process such as obtaining an airworthiness certificate stating that the system meets the required level of safety. It is therefore important that the reported data and estimates for a particular vehicle be accurately reported. This is further reinforced by the seventh statement of the IEEE Code of Ethics, which states the expectation for the accurate acknowledgement and response to off-nominal operations. It states that its members agree ``to seek, accept, and offer honest criticism of technical work, to acknowledge and correct errors, and to credit properly the contributions of others"[13].

The fifth statement of the IEEE Code of ethics reads that its members agree ``to improve the understanding of technology; its appropriate application, and potential consequences", and the tenth ethics statement states its members agree ``to assist colleagues and co-workers in their professional development and to support them in following this code of ethics" [13]. This statement clearly articulates the need of educators teaching unmanned systems to explicitly address within their curriculum and through faculty advisement the technological applications of

unmanned systems, their current regulations, and a discussion of any ethical debate associated with their engineering and usage.

The ninth statement of the IEEE Code of ethics reads that its members agree ``to avoid injuring others, their property, reputation, or employment by false or malicious action" [13]. This can be interpreted as relevant to the public safety concerns. It also reinforces the importance of lawful operation of unmanned systems, which must be ensured when students are involved in extracurricular activities within the unmanned systems domains.

As discussed earlier within this document, AUVSI, the trade organization for unmanned systems, provides in place of a code of ethics a "code of conduct"[10]. The AUVSI Unmanned Aircraft System Operations Industry Code of Conduct is divided into three sections: safety, professionalism, and respect. Safety focuses upon guidelines to ensure safe operation of the UAS within the national airspace system, which aligns with the expectation for engineers to ensure safety, health, and public welfare. Professionalism focuses upon legal operation, disclosure of mishaps/accidents, responsiveness to public concern, and appropriate contingency planning to mitigate the impact of the public of a system fault/failure. Lastly, respect under the code of conduct calls to respect privacy, respect for public concern, and support the education of the public.

4.2 Incorporating Unmanned Systems Ethics into the Curriculum

For the new MSUASE program, many of these issues are currently being incorporated into the course ME 503: Introduction to Unmanned Systems, which is required during the first term for students admitted for the fall semester. For the Fall 2013 offering, collaboration between students in ME 503 and students at the University of Washington Law School was established. Engineering students at Embry-Riddle Aeronautical University addressed technical questions fielded by students from the University of Washington, and the University of Washington students addressed policy questions addressed to them. Both groups then discussed their respective response creating a mutual dialog and encouraging discussion regarding the responses and counter-arguments of each group.

Topics discussed with respect to unmanned aircraft and/or driverless cars include:

- Who is responsible for creating regulations to ensure public safety, and who ensures that these regulations are followed?
- Who is responsible in the event of an accident/mishap?
- How is data secured and maintained?
- Can an unmanned system be hacked, and what implications would this have on the market?
- To what extent are privacy fears justified? How will this mindset evolve?

As the program matures, additional ethics related content must be incorporated into the curriculum.

At the undergraduate level, ethics related to unmanned systems is explicitly discussed in the ECSSE Department's capstone design course. Each student team must produce an ethics paper

that both addresses the ethical issues/dilemmas that could result from the unmanned technologies being produced as part of their design project. Students additionally must review each of the IEEE Code of Ethics guidelines and state its applicability to their project and role within the project.

5.0 Dissemination of Technical Information Related to Unmanned Systems

The issue of safe and legal dissemination of technical information and access to technologies associated with unmanned systems is a major concern that must be addressed for any unmanned systems program. To facilitate an academic program in unmanned systems engineering, it is expected that students will be working on sponsored, curricular, or co-curricular projects. This is an important ethical requirement as it relates to public health and safety directly.

Projects involving industry are often associated with a non-disclosure agreement. These agreements are commonplace within academia and industry, and can often been executed by the appropriate signatory authorities. Maintaining compliance with the agreement is the obligation of the participants. As such, it is important that faculty advisors / instructors adequately educate student participants regarding such agreements and the implications of the terms within those agreements.

Projects with the Department of Defense, or defense contractors, can be deemed classified, secret, or even higher security classifications. Working with such technologies, software, and/or documents can require significant overhead including security clearances.

An area of some confusion and common concern within academia is the issue of meeting restrictions on the dissemination of information regarding unmanned technologies based upon risk to national security. This includes International Trade in Arms Regulations (ITAR)[16] and Export Administration Regulations (EAR)[17] restrictions on the access or export of goods to non-US persons, non-US corporations, and foreign entities. This is often a gray area for many as technological goods, knowledge, software etc. can fall under what is considered ITAR or Export Controlled, and could face harsh penalties and/or jail time for violation of these regulations.

This remainder of this section will focus upon ITAR and EAR concerns. However, as a necessary disclaimer, the authors are providing a general overview. It is up to those involved in such research and education activities, and their appropriate legal compliance designee to ensure that they are meeting these regulations. Likewise, the U.S. export control agencies place the onus of universities to understand and comply with the regulations.

5.1 ITAR

ITAR restrictions are maintained by the United States Department of State's Directorate of Defense Trade Controls in accordance with Title 22 Code of Federal Regulations (CFR) Parts 120-130 (known herein as simply ITAR), which controls the export and temporary import of defense articles[16]. The United States Munitions List (ITAR 121.1) defines the articles and services restricted under these terms[18]. In general, restrictions must be established such that in no way an ITAR controlled item/technical data is transferred, made available to, or distributed in

the following way: to a foreign person employed by the university, residing within the United States, or outside the United States; and for an end-use not included in the State Department authorization.

Under ITAR120.17, the term “Export”" is defined. It includes the sending of a defense article outside the United States; transferring ownership, registration, or control to a foreign person, within the US or outside of the US, of a USML restricted item; disclosing or transferring defense articles to a foreign embassy or government entity; disclosing or transferring a defense article to a foreign person; performing a defense service for or on behalf of a foreign national; etc.

The definition of items controlled by ITAR is quite broad. It can be defined as a defense article (ITAR 120.6), technical data (ITAR 120.10), and defense service (ITAR 120.9). A defense article is an item or technical data identified under the USML (ITAR 121.1)[19]. Technical data more broadly defined to include information necessary for the design, development, production, operation, repair, etc. of a defense article including blueprints design documents, operations manuals, etc[19]. Technical data produced within the public domain, including fundamental research at universities that would be typically published and broadly disseminated is exempt[19]. Lastly, a defense service is defined as the furnishing of assistance (including training) to a foreign person in the design, development, engineering, manufacturing, etc. of a defense article; furnishing a foreign person with any ITAR restricted technical data, or military training[19].

In an academic setting, there are both obvious and non-obvious items to which the definition above is applicable. For instance, the Piccolo autopilot[20] is an ITAR restricted component that is commonly used for unmanned aircraft. Not only is the physical device restricted, but also so are its technical data including any source code and any documents not designated for public release. For a less obvious case, thermal-imaging cameras such as those produced by FLIR may fall under ITAR control if they have frame rates greater than 9Hz and a resolution of 640x480 or higher[21]. If it is uncertain whether an item, technical data, or service falls under ITAR control, it is the responsibility of the faculty member and/or organization to request a Commodity Jurisdiction determination from the Directorate of Defense Trade Controls at the U.S. State Department.

5.2 Export of Dual-Use Goods and Technology

Under the Export Administration Regulations (EAR)[17], dual-use items are items that can be used both in the military and other strategic uses and in civil application (versus weapons, which fall under ITAR). The purpose of these export controls is to prevent access to dual-use technologies to countries or persons intent on doing harm to the United States and its interests[17]. Export is defined broadly and also includes the “release of a technology to a foreign national in the United States through such means as demonstration or oral briefing”[17].

5.3 Potential Compliance Practices

The compliance with ITAR and Export Control regulations should be addressed at the university level with clear policies established to protect faculty, students, staff, and the institution. This sub-section briefly describes some of the practices in place to ensure compliance at the author's

institution. The university must be vigilant in following up upon any suspicious inquiries or violations of ITAR policy.

For projects working with ITAR/EAR restricted materials and technical data, participation must be limited to U.S. Persons as defined in ITAR 120[19] with proof of citizenship/naturalization. A registration of project participants must be maintained for access control to any ITAR restricted classroom or laboratory. A laboratory manager must ensure positive ID of all entrants into the laboratory, and any foreign nationals must be escorted. Citizenship must be verified before the sharing of any export controlled materials within the lab. All persons working within the ITAR controlled space must be adequately briefed on ITAR policies and sign the University's ITAR non-disclosure form.

ITAR controlled items must be clearly identifiable. The item should be labeled "ITAR Export-Controlled". If the item is of text form, the first page of technical data shall be marked as follows:

> This document contains technical data within the definition of the International Traffic in Arms Regulations (ITAR) and is subject to the export controls laws of the US government. Transfer of this data by any means to a foreign person or foreign entity, whether in the United States or abroad, without an export license, ITAR exemption or other approval from the US department of state, is prohibited.

Each subsequent page must be labeled as: "This document is subject to the controls and restrictions specified on the first page".

ITAR/EAR controlled items must be adequately secured to prevent unauthorized export. At a minimum, our ITAR restricted labs require swipe access for entry. The rooms are interior without any external/non-secure window. Smaller items (e.g. cameras, sensors, components, data manuals, etc.) are placed in a locked cabinet or safe. Digital materials must be stored within the ITAR controlled room under an approved export compliant computer. Print technical data is only printed on non-network printers.

An inventory of all ITAR/EAR controlled materials must be maintained. A weekly inventory is performed to ensure all restricted items are accounted. Printer materials deemed ITAR controlled, but no longer in use will be shredded to assist in maintaining positive control on all technical data.

Lastly, access to service providers such as janitorial staff, maintenance personnel, etc. must also be considered. Such personnel must provide adequate documentation as defined under ITAR 120.15[19]. Similarly, those persons must be briefed and required sign an ITAR non-disclosure form making them aware of university policy regarding the handling of these restricted items.

6.0 Conclusion

Academic curricula and research within the area of unmanned systems is not without some ethical concerns and/or issues that must be addressed or at least communicated with the academic community. These concerns include the adherence to a professional Code of Ethics to

ensure the ethical, legal, and safe engineering of such systems. A number of ethical issues have been identified that must be discussed within the curriculum to educate students to inform their personal/career decisions. Lastly, the technologies utilized and/or developed in this research can fall under U.S. government restrictions such as ITAR or EAR to mitigate the risk of these technologies being acquired and used for purposes that threaten the safety and health of the public.

7.0 References:

[1] Arkin, R.C. On the Ethical Quandaries of a Practicing Roboticist: A First-Hand Look. In Proceedings of the 2008 conference on Current Issues in Computing and Philosophy, Adam Briggle, Katinka Waelbers, and Philip A. E. Brey (Eds.). IOS Press, Amsterdam, The Netherlands, The Netherlands, 45-49, 2008.

[2] Arkin, R.C., "Governing lethal behavior: Embedding ethics in a hybrid deliberative/reactive robot architecture part I: Motivation and philosophy," *Human-Robot Interaction (HRI), 2008 3rd ACM/IEEE International Conference on*, vol., no., pp.121--128, 12-15 March 2008.

[3] Arkin, R.C., *Governing Lethal Behavior in Autonomous Systems*, Taylor and Francis, 2009.

[4] Sparrow, R., ""Just Say No" to Drones," *Technology and Society Magazine, IEEE*, vol.31, no.1, pp.56, 63, Spring 2012
doi: 10.1109/MTS.2012.2185275

[5] Veruggio, Gianmarco. "EURON Roboethics Roadmap", EURON Roboethics Atelier, 27 February - 3 March 2006 (Accessed online at http://www.roboethics.org/atelier2006/docs/ROBOETHICS%20ROADMAP%20Rel2.1.1.pdf, 3 January 2014).

[6] U.S. Government Printing Office, "FAA Modernization and Reform Act of 2012 49 USC 40101" (Accessed online at http://www.gpo.gov/fdsys/pkg/PLAW-112publ95/pdf/PLAW-112publ95.pdf, 4 January 2014), 14 February 2014.

[7] U.S. Federal Aviation Administration. Fact Sheet – Unmanned Aircraft Systems (UAS), (Accessed online at http://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=14153 , 4 January 2014), 19 February 2013.

[8] American Civil Liberties Union, "Protecting Privacy from Aerial Surveillance: Recommendations for Government Use of Drone Aircraft" (Accessed online at https://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf, 4 January 2014), December 2011.

[9] Association for Unmanned Vehicle Systems International. "Comments of the Association for Unmanned Vehicle Systems International on the Aerospace States Association Suggested Privacy Legislation Plan 2013". (Accessed online at: http://aerostates.org/wp-content/uploads/AUVSI-Comments.pdf, 3 January 2014), 1 June 2013.

[10] Association of Unmanned Vehicle Systems International. Unmanned Aircraft System Operations Industry "Code of Conduct". (Accessed online at http://www.auvsi.org/conduct, 4 January 2014), August 2012.

[11] International Association of Chiefs of Police. "Recommended Guidelines for the use of Unmanned Aircraft". (Accessed online at http://www.theiacp.org/portals/0/pdfs/iacp_uaguidelines.pdf, 4 January 2014).

[12] Federal Aviation Administration. "Final FAA Privacy Policy for UAS Test Sites" (Accessed online at http://www.faa.gov/about/initiatives/uas/media/UAS_privacy_requirements.pdf, 4 January 2014), 2013.

[13] International Electrical and Electronics Engineers. "7.8 IEEE Code of Ethics". (Accessed online at http://www.ieee.org/about/corporate/governance/p7-8.html, 4 January 2014).

[14] ASME Standards Technology, LLC. "Code of Ethics of Engineers". (Accessed online at http://files.asme.org/STLLC/13093.pdf, 4 January 2014), 9 October 2007.

[15] American Institute of Aeronautics and Astronautics. "AIAA Code of Ethics". (Accessed online at http://www.aiaa.org/SecondaryTwoColumn.aspx?id=19693, 4 January 2014).

[16] United States Department of State, "International Traffic in Arms Regulations (ITAR)". Directorate of Defense Trade Controls (Accessed online at http://www.pmddtc.state.gov/regulations_laws/itar.html, 4 January 2014).

[17] Department of Commerce. "Export Administration Regulations (EAR)". (Accessed online at http://www.bis.doc.gov/index.php/forms-documents/doc_view/410-part-730-general-information, 4 January 2014), 15 October 2013.
[18] United States Department of State, "Title 22 Code of Federal Regulations Part 121 – The United States Munitions List". (Accessed online at http://www.pmddtc.state.gov/regulations_laws/documents/official_itar/2013/ITAR_Part_121.pdf, 4 January 2014).
[19] United States Department of State, "Title 22 Code of Federal Regulations Part 120– International Traffic in Arms Regulations". (Accessed online at http://www.pmddtc.state.gov/regulations_laws/documents/official_itar/2013/ITAR_Part_120.pdf, 4 January 2014).
[20] CloudCap Technologies. "Product Export Facts Document", (Accessed online at https://www.cloudcaptech.com/Sales%20and%20Marketing%20Documents/Product%20Export%20Facts.pdf, 5 January 2014), 2012.
[21] FLIR. "Knowledge Base: Is an export license required for Tau and Quark thermal imaging cameras?". (Accessed online at http://www.flir.com/cvs/cores/knowledgebase/index.cfm?CFTREEITEMKEY=342&view=35781, 4 January 2014).