A9 - Legal and Regulatory Analysis

Year: 2024 Semester: Spring Team: 2 Project: MOUSE

Creation Date: ­ March 18, 2024 Last Modified: March 23, 2024

Author: Braden Kirkendall Email: bkirkend@purdue.edu

1.0 Regulatory Analysis

The FCC oversees defining and upholding regulations involving signals occurring within the frequency range of the electromagnetic spectrum. They do so to prevent interference between commercial devices and ensure efficient use of communication channels.

Under FCC guidelines [4], the 48 MHz frequency of the ESP32S3 microcontroller core contained within the MOUSE is subject to the classification of “Unintentional radiators” as outlined in Part 15, subpart B due to its operating frequency between 9 kHz and 3000 GHz and its commercial availability for public or private use. This means that before entering the market, the MOUSE must be validated to ensure accordance with the guidelines set by the FCC as established by the Supplier’s Declaration of Conformity procedure. These validation tests include the following [5]:

* “A detailed test report of formal EMC measurements demonstrating that your product meets either Class B or Class A Part 15 EMI limits.”
* “Formal chamber testing will include both Radiated Emissions & Conducted Emissions”
* “Your product manual must have the required regulatory language and warnings to inform users that your product meets FCC Part 15 limits.”
* “As a new addition under the SDoC, your product manual also must contain a compliance statement which identifies the responsible party of the product who can be contacted for any FCC compliance needs in the future”
* “Under the SDoC, your product may be labelled with the FCC Logo and should have a product label with a model number that consumers can uniquely identify your product from.”

Additionally, the FCC guidelines designate the DC motors contained within the MOUSE to be an “Incidental Radiator” under Part 15, subpart A since it does not “intentionally generate or intentionally emit radio frequency energy over 9 kHz.” However, it “may produce byproducts or radio emissions above 9 kHz and cause radio interference.” Under the Supplier’s Declaration of Conformity this means that it is subject to be tested in the same fields as previously discussed for class B radiators as a part of FCC Part15B testing. One key detail is that the ‘B’ in the testing protocol is not a class indicator and that this test is performed on both class A and B radiators. Only after this testing has been performed can the MOUSE be brought to market.

In addition, one use case for the MOUSE surveillance robot is in classified spaces at defense companies. To be implemented, the MOUSE should adhere to regulations from agencies including but not limited to the Department of Defense, the Central Intelligence Agency, and the National Security Agency that dictate the use of technology in these classified spaces. In addition, the MOUSE should be aware of the internal policies put in place by major companies restricting surveillance devices. While not necessary, something that would give MOUSE an edge in the market is government approval to be used in classified areas. However, to get this approval it is likely that the webserver-based communication would need to be modified as device access to Bluetooth and Wi-Fi is restricted in these areas.

While the MOUSE itself does not transfer specific classified information, the ability to maneuver and view the logged information should abide by regulated cybersecurity standards to prevent unauthorized access to the controls or data logs. Some common examples of such standards include NIST SP 800-53 and ISO/IEC 27001 and they outline key implementation details to ensure data protection [6].

These standards require that the MOUSE have an implemented “Access Control” layer which acts as a secured login system to verify the identity and authorization level of each user. For our prototype, this would involve creating a cryptographically secure account system with a user database. The system would have to be verifiably secure through penetration testing and security audits to bring to market successfully. An added layer of security that MOUSE provides is that the data it contains is not directly related to the contents of classified information, however effective security measures should still be in place.

Cybersecurity standards also hold requirements regarding the ability of the product to become alert of and respond accordingly to breaches of security. This also closely ties with network systems protections for digital traffic and communication encryption. In order for the MOUSE to meet these standards, its messaging system should include encryption to improve security. This would involve configuring both the webserver and the microcontroller to incorporate the advanced encryption standard. Additionally, if a security breach occurs, the system should have internal alerts of suspicious behavior. This would involve adding a new system state where message receiving and sending is locked down until high authority credentials are used or potentially even wiping the data in extreme circumstances.

2.0 Legal Liability Analysis

2.1 Analysis of Patent 1

US Patent Application US7436143B2 [1]:

Patent Title: “Miniature surveillance robot”

**Patent Holder:** M Bots Inc

**Patent Filing Date:** April 25, 2006

**Abstract: “**A robotic system has a drive chassis having a drive motor and a drive element attached to the first drive motor. Additionally, a motor controller system provides drive signals to the first drive motor. A logic controller provides control signals to the motor controller. A network system is provided for communicating with the logic controller. At least one peripheral element communicates with the network system. There is additionally provided a wireless arrangement for communicating wirelessly with the network system.”

A diagram of a machine

Description automatically generated

**Figure 1. Miniature Surveillance Robot Design**

Potential Infringements:

Among the claims, the MOUSE potentially infringes upon the following:

* A robotic system, comprising: a drive chassis having a first drive motor; a first drive element attached to said first drive motor; a motor controller system for providing drive signals to said first drive motor; a logic controller for providing control signals to said motor controller; a network system for communicating with said logic controller; a peripheral element for communicating with said network system; and a wireless arrangement for communicating wirelessly with said network system, said wireless arrangement being configured to propagate drive actuation signals from a remote drive control source to said logic controller
* The robotic system of claim 1, wherein said first element comprises a wheel
* The robotic system of claim 1, wherein said peripheral element communicates with said network system using Transmission Control Protocol (TCP)
* The robotic system of claim 1, wherein said peripheral element is a proximity sensing system

The MOUSE shares a lot of design features in common with the Miniature Surveillance Robot Design. In the first claim, there is overlap in the drive chassis, drive motor, motor controller system, and logic controller. While there are also similarities in the incorporation of a peripheral element to monitor and communicate wirelessly with the robot, there are some differences in the implementation of our design. The patented design uses the peripheral as the external communication device that transmits data to the logic controller over the network whereas our design directly connects our proximity sensor peripheral to the logic controller directly. Our implementation of the network is for the user dashboard that controls the MOUSE itself rather than directly communicating sensor data with network packets and TCP. For this reason, it could be argued that the implementation is not infringing upon the intellectual property in this patent as the same materials are being used in a different functional configuration. Additionally, this patent has since been expired.

* 1. Analysis of Patent 2

US Patent Application US20220157137A1 [2]:

Patent Title: “Facility surveillance systems and methods”

**Patent Holder:** Hexagon Technology Center GmbH

**Patent Filing Date:** December 23, 2021

**Abstract:**

“Systems and methods for surveillance of a facility including facility elements. The system includes a central computing unit providing a digital model of the facility providing topological or logical or functional relationships of the facility elements, surveillance sensors adapted for surveillance of a plurality of the facility elements and for generation of surveillance data, communication means for transmitting data from the surveillance sensors to the central computing unit, and state derivation means configured to analyze the surveillance data and derive a state of a respective facility element. The central computing unit is configured to record a state pattern by combining states of at least one facility element based on at least one relationship of the facility element provided by the facility model, provide a state pattern critical-noncritical classification model which considers relationships provided by the facility model, and perform a criticality-classification based on the relationship.”

A diagram of a house

Description automatically generated

**Figure 2. Facility Surveillance System and Methods**

Potential Infringements:

Among the claims, the MOUSE potentially infringes upon the following:

* The mobile surveillance system adapted for patrolling a surveillance area of a facility, particularly of a building, the system comprising a plurality of sensors, in particular comprising at least two cameras, wherein the system comprises at least one unmanned ground vehicle (UGV) that is adapted to move autonomously on a ground of the surveillance area, the UGV comprising a housing enclosing:

a first battery;

first sensor means, particularly comprising a first camera, the first sensor means being adapted to generate first sensor data,

a first computing unit comprising a processor and a data storage, the first computing unit being adapted to receive and evaluate the first sensor data in real time,

wherein the system comprises at least one unmanned aerial vehicle (UAV), the UGV and the UAV being adapted for collaboratively patrolling the surveillance area, wherein:

the UAV comprises second sensor means, particularly comprising a second camera, the second sensor means being adapted to generate second sensor data,

the UGV comprises a first data exchange module and the UAV comprises a second data exchange module, the first and second data exchange modules being adapted to exchange data; and

the first computing unit is adapted to receive and evaluate the second sensor data in real time.

* The mobile surveillance system according to claim 1, wherein the computing unit is adapted to generate UGV controlling data for controlling functions of the UGV in real time and based on the evaluation of the first sensor data.

Relative to the MOUSE this patent incorporates many claims in the area of scaling large-scale systems of vehicles, which trivially does not apply to MOUSE’s single-vehicle implementation. When identifying the corresponding characteristics that define an unmanned ground vehicle, MOUSE fits many of the descriptors. Notably it has real-time data processing capabilities from its sensor peripheral and relays data to a central computing unit to dictate control of the vehicle. The defense of the MOUSE in not infringing upon these claims lies in the difference in mechanisms used to accomplish surveillance. The patent uses a horde of unmanned vehicles and uses a collective pool of data to allow autonomous movement behavior. This is well beyond the scope of the MOUSE’s semi-autonomous implementation goal and there is no aerial vehicle component to our design. Furthermore, the specification is specific to generating a design which uses at least two cameras. This qualification is not met by the MOUSE.

* 1. Analysis of Patent 3

US Patent Application US4638445A [3]:

Patent Title: “Autonomous Mobile Robot”

**Patent Holder:** Paul J. Mattaboni

**Patent Filing Date:** Jan. 20, 1987

**Abstract:**

“A vision system for a mobile robot employs at least two arrays of sensors for obtaining data on the position and distance of objects in a workspace. One of the sensor arrays is used principally to see near objects and the other array is used principally to see far objects. The two arrays are symmetric about an axis that extends through the body of the robot. The robot carries a computer which controls the sequence in which the sensors are serially polled for information. Data received from the sensors is stored and provides a representation of the space and objects seen by the sensors. A software program causes the computer to manipulate data from the sensors to simulate rotation of the robot around the axis of symmetry and control behavior of the robot to complete goals set by input commands from a natural language processor.”

A drawing of a machine

Description automatically generatedA drawing of a machine

Description automatically generated

**Figure 3. Autonomous Mobile Robot by Paul J. Mattaboni**

Potential Infringements:

Among the claims, the MOUSE potentially infringes upon the following:

* In a mobile robot of the type having

(a) a vision system,

(b) memory means for storing data derived from the robot vision system, and

(c) a computer for processing data derived from the robot's vision system

the improvement wherein the robot's vision system comprises:

1. a first array of ranging transducers for obtaining data on the position and distance of far objects in a volume of space, the transducers of the first array being symmetrically disposed on the mobile robot with respect to an axis of symmetry within the mobile robot, each transducer of the first array being fixed in position with respect to that axis of symmetry and seeing a portion of the volume of space seen by its entire array.

(ii) a second array of ranging transducers for obtaining data of the position and distance of near objects in the same or an overlapping volume of space, the transducers of the second array being symmetrically disposed on the mobile robot with respect to said axis of symmetry, each transducer of the second array being fixed in position with respect to said axis of symmetry and seeing a portion of the volume of space seen by its entire array, the angle of view of the transducers of the second array being different from the angle of view of the transducers of the first array with respect to the same object in space; and

(iii) means for polling said ranging transducers in sequences determined by the computer.

There are similarly inspired solutions to the problem of moving a robot autonomously that overlap between this patent and the MOUSE, however the implemented details in the patent are much more specific and precise that what is able to be attained in our design. While MOUSE’s sensor peripheral system could rudimentarily be categorized as a vision system and MOUSE has memory storage and computer-based data processing. Yet, the transducer array used for spatial recognition and algorithmic reasoning exceeds the scope of our project. MOUSE does not create an array to organize its layout from its scanning of the environment and its scanning system is solely for movement detection rather than precise autonomous functionality.

3.0 Sources Cited:

[1] B. Metzler et al., “US20220157137A1 - facility surveillance systems and methods,” Google Patents, <https://patents.google.com/patent/US20220157137A1/en?q=%28autonomous%2Bsurveillance%29&oq=autonomous%2Bsurveillance> (accessed Oct. 15, 2023).

[2] S. Lakshmanan, V. J. Varghese, and N. Natarajan, “US7436143B2 - Miniature Surveillance Robot,” Google Patents, <https://patents.google.com/patent/US7436143B2/en?q=%28surveillance%2Brobot%29&oq=surveillance%2Brobot> (accessed Oct. 15, 2023).

[3] P. J. Mattaboni, “US4638445A - Autonomous Mobile Robot,” Google Patents, https://patents.google.com/patent/US4638445A/en (accessed Oct. 15, 2023).

[4] “Equipment Authorization – RF Device,” *Federal Communications Commission*, Dec. 08, 2015. <https://www.fcc.gov/oet/ea/rfdevice>

[5] “What Is FCC Part 15 Testing?,” *sunfiretesting.com*. https://sunfiretesting.com/What-Is-FCC-Part-15-Testing/#:~:text=What%20is%20an%20unintentional%20radiator (accessed Mar. 23, 2024).

[6] NIST, “Security and Privacy Controls for Information Systems and Organizations,” *csrc.nist.gov*, Dec. 10, 2020. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final