ECE4011/ECE 4012 Project Summary

Project Title	Infantry IFF (Identification Friend-or-Foe) System
Team Members (names and majors)	Vijay Krishnan, CmpE Kevin Waddles, EE Donghoon Han, EE Vishal Devidas, CmpE Rishabh Patel, CmpE
Advisor / Section	Dr. Tentzeris/L06A
Semester	Fall 2019 **Final (ECE4012)**
Project Abstract (250-300 words)	Identification of friendly assets in the chaos of war continues to be a challenge in modern day military operations. The lack of a reliable method to distinguish armed forces has led to rising instances of fratricide, or the accidental killing of allied soldiers. Over the past century, RF technology has led to the creation of IFF (identification friend-or-foe) systems; however, most systems are only implemented in aircrafts and vehicles. This valuable piece of technology has yet to make its way into the hands of infantry soldiers, who are arguably in need of it the most. The team's objective is to build **a low power, durable, and lightweight IFF system** that can be used by infantry soldiers on the battlefield. Weapons carried by soldiers are to be fitted with transceiver units capable of sending out frequency modulated RF signals over a large range. A separate bluetooth enabled processing unit is fitted on allied soldiers to broadcast a 2.4 GHz signal to retrieve the position of the surrounding soldiers. Allied soldiers are also fitted with reflector badges that incorporate the back-scatter reflector array technology. When a soldier points his or her weapon towards an ally, a 24GHz RF signal is sent from the interrogator towards the target. If the target is an ally and is wearing the reflector badge, the signal is sent back to the interrogator, alerting the user that the target is a friendly. The project will examine various tradeoffs between functionality and miniaturization; it will also enhance the combat capabilities of each soldier so that missions can be completed as efficiently and quickly as possible.

Project Title	Infantry IFF System
List **codes** and **standards** that significantly affect your project. Briefly describe how they influenced your design.	- False positives: Ensuring that signals received by the transmitter are not rejecting a true positive signal or accepting a false signal. - Proper RF frequencies: Ensuring the system complies with National/International Standards of frequency channels - Secure Encryption/Decryption: Using a highly sophisticated cryptographic algorithm to keep transmission from being intercepted. - USB: needed to interface between the Radar GUI and the FMCW board. - IEEE 802.11: needed for wireless communication via bluetooth in the processing units mounted on each allied soldier.
List at least two significant **realistic design constraints** that applied to your project. Briefly describe how they affected your design.	- Cost: the limited allocated budget restricted us to use FMCW transceiver units with limited range (maximum range of 25 m). - Accuracy of the reflected signal from the reflector badge on the target with ±2 degrees of deviation. - Transmitting the signal from source with a 140-degree range makes it difficult for the sender to distinguish the signals reflected back from multiple targets present in the 140-degree area range.
Briefly explain two **significant trade-offs** considered in your design, including options considered and the solution chosen.	- Angle of transmission vs. precision of reception. We would like to limit our system's transmission angle so that enemy detectors cannot see the transmitter's position. This will affect the precision of reception such that our receiver must perform very well. - Cost vs. range of the transmitted RF signal: the position2go FMCW radar is within our budget but it offers a maximum range of 25 m. An alternate FMCW radar offering extended range of over 100 m is well outside the budget. While the range is increased, transmitting the signal over 100 m with a 140-degree range would make it difficult to distinguish it from other transmitted signals.
Briefly describe the **computing aspects** of your projects, specifically identifying **hardware-software** tradeoffs, interfaces, and/or interactions. *Complete if applicable; required if team includes CmpE majors.*	**Hardware** The RF response is generated by a back-scatter reflector array patch antenna for low power consumption and weight. All the hardware components are mounted on a protoboard for ease of modification along with the transmitter. **Software** A transmitted bluetooth signal would need to be encrypted using an encryption algorithm. A front-end user interface may also be necessary to monitor signal detection and reception. **Trade-offs** One important trade off on the software end will be deciding between encryption algorithms with respect to optimizing encryption/decryption time, memory usage and the number of physical bits necessary for successful encoding.