ECE4871/ECE 4872 Project Summary

Project Title	Azure Zero Trust IoT Network (Boeing – Team 8)
Team Members (names and majors)	Noah Dorfman - CompE Zixuan Kang (Harry) - CompE James Thomas - CompE Aaron Wasserman - CompE Jayla Williams - CompE
Advisor / Section	Dr. Brendan Saltaformaggio
Semester	2021/Spring Circle: ECE4871
Project Abstract (250-300 words)	One of the most challenging aspects of analytics, data science and machine learning is getting quality data. This project focuses on setting up a stringently secured network of IoT devices that push data to the cloud where it can be accessed for analysis. Our team will implement a Microsoft Azure Zero Trust connection between several Nordic microcontrollers using Arm Cortex-M3 chips sRF52840, nRF9160, or nRF52832) and Azure Data Lake for data collection. The network will be implemented using BLE and will require a gateway device to the Azure IoT Broker. The devices connections will be implemented over a BLE mesh network. There are limited Zero Trust IoT solutions on the market today, which makes such a system valuable in IoT settings where security is of utmost priority. Our goal is to successfully program, install, and test our Nordic-based system and show complete and operation by recording data from the IoT sensors connected to the microcontroller and storing it on the remote server. With this functionality achieved, it is possible to demonstrate the security by conducting various network, software, and hardware-based attacks against our implementation. This will include testing the effective protection against backdoor intrusions such as wired taps through analog or digital IC connections capture sensor data input to the microcontroller. We will examine the potential to corrupt the Zero Trust protection through power input irregularities using methods like glitching, also known as voltage fault injection, to cause corruption to instructions that could result in bypassed security checks. Our team will also be analyzing the implementation for susceptibility to side channels attacks like power analysis and timing attacks. Using fuzzing and industry-leading vulnerability scanners to verify the security of the software, we will prove the security of our code and network architecture.

Project Title	Azure Zero Trust IoT Network (Boeing – Team 8)
List **codes** and **standards** that significantly affect your project. Briefly describe how they influenced your design.	MQTT standard will be used for transmission to the Azure IoT Hub. BLE will be used for the mesh network. Authentication will be required when each node access the database or cloud services and when a new device is trying to connect to the network.
List at least two significant **realistic design constraints** that applied to your project. Briefly describe how they affected your design.	Nordic Devices will come with the appropriate sensors and transmission hardware needed for the Bluetooth mesh network. Azure IoT Hub protocols being limited to MQTT or AMQP over web sockets. The project will rely on MQTT for the transmission of data to Azure IoT Central with the endpoint of Azure Data Lake Storage. For a more robust solution, Azure IoT protocol Gateway can be used to accept MQTT and bridge connections to IoT Hub with AMQP.
Briefly explain two **significant trade-offs** considered in your design, including options considered and the solution chosen.	Server communication medium: LTE on the Thingy 91 vs. Separate gateway device Pros of using LTE on Thingy 91 • Lightweight system (eliminate the need for extra devices) • useful everywhere with a cellular connection • Security less complicated Pros of using separate gateway (RPi) • Initialization is easier. • More existing community support • More versatile • Allows for more complicated tasks to be completed. • Useful for future applications (doing work on the network edge, rather than going to the server for everything) IoT Protocol: AMQP vs. MQTT AMQP • Can be more secure. • More configurable • For Azure, AMQP is needed for using their service endpoints • For Azure, Microsoft offers various security features with AMQP MQTT • Low overhead • Simple to implement and send data from embedded systems. • Best for many small messages on low-bandwidth networks • For Azure, MQTT works well with Azure Data Lake Storage • For Azure, IoT Protocol Gateway offers a way to bridge to AMQP if a service offering from MS is required

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.*	Interfacing with Azure IoT Hub will be required, which is numerous cloud computing microservices for collecting, analyzing, and pushing data to and from embedded devices. When compared with Google IoT Core, the pricing is more reasonable as the pricing model for google was paying per trigger on each message. The Azure IoT Hub requires specific messaging transmission protocols, the most popular being MQTT.

Project Title	Azure Zero Trust IoT Network (Boeing – Team 8)
Leadership Roles (ECE4871 & Forecasted for ECE4872) (NOTE: ECE4872 requires definition of additional leadership roles including: 1.Webmaster 2. Expo coordinator 3. Documentation	4871 Leadership Roles: Jayla Williams - Networking Lead Aaron Wasserman - Hardware Security Testing Lead Noah Dorfman - Documentation, Embedded Hardware Lead James Thomas - Advisor point of contact, Azure IoT Software Lead Harry Kang - Boeing point of contact, Zero Trust Architecture Consultant, Embedded Software Lead 4872 Leadership Roles: Jayla Williams - Webmaster, Networking Lead Aaron Wasserman - Expo Coordinator, Hardware Security Testing Lead James Thomas - Azure IoT Software Lead Noah Dorfman - Documentation, Embedded Hardware Lead Harry Kang - Implementation Testing, Embedded Software Lead
International Program: Global Issues (Less than one page) (Only teams with one or more International Program participants need to complete this section)	n/a