Vehicle to Vehicle - Requirements

Erik Kamph*
Email: *ekh17001@student.mdh.se
Mälardalens University Solar Team - Electronics domain - November 17, 2020

I. Document Overview

This document presents requirements for the vehicle to vehicle communication system. This includes requirements not only for the antenna and physical signals, but for reliability and redundancy, security and communication as well.

II. Purpose of this document

The purpose of this document is to present all the different requirements for hardware as well as the software when it comes to vehicle to vehicle communication. This is done in order to determine what hardware we need for vehicle to vehicle communication. This means that we need to specify requirements that deal with reliability, reduncancy, package-loss etc. We need to specify requirements based on regulations from European Union and Australian government for radio devices. We also need to specify requirements from Bridgestone World Solar Challenge 2021 Regulations.

III. Requirement specification

Following is sections that list the requirements for the different devices, requirements for reliability as well as communication requirements.

A. Requirements for antenna and signal strength

- The minimum range for the connection while using an antenna shall be at least 100 meters.
- The selected antenna must be certified for use within both Europe and Australia when it comes to signal and frequencies, if not possible it should at least
  - be an antenna that is certified within EU for use when testing, and
  - later a new antenna must be selected that is certified for use in Australia that has the similar characteristics as the one found in EU.
- If possible the antenna shall limit the area of communication to behind the car creating a cone-formed beacon big enough for turns and corners when driving.

B. Reliability

- There should be a cryptography method that does not impact transfer speed of packages or performance of the device.
- Packages received must be verified and shall be
  - disposed if they are corrupted, but
  - decrypted if the packages have not been tampered with.
- The receiver should be able to verify the sender by the connection.
- Package-loss shall be detected
  - with cryptography or a cyclic redundancy check to see if they were corrupted
  - when it takes too much time to receive packages after a number of retries
  - when out-of-range from the supporting follow vehicle.
- When package-loss occurs the sender shall have a small buffer for packages that is used for re-sending the packages when it has connection.

C. Communication

- It should be possible to extend BLE packages with additional data other than messages coming from the CAN.
- It needs to be able to write and read data from the CAN bus.
- Each device needs to send its connection status to their respective local storage.

D. Connection specification

- The sender should be able to transfer data to the receiver faster than getting getting data from CAN to minimize congestion.
- The receiver should be able to receive data equally fast as the sender sends it in order to minimize congestion.
- The sender shall make use of the buffer specified under Reliability in case of a connection loss.
- During a connection loss the sender shall dispose packages that there are multiples of or packages that have been in the buffer for to long.