This thesis deals with description of CRC codes, which is a type of polynomial error correction codes, and description of CAN and CAN FD protocols used in automobiles for data transmission between sensors. One of the security elements is usage of the CRC codes with the Hamming distance 6. Unfortunately, both protocols contain a design vulnerability which causes that some received messages with one wrong bit do not have to be detected by the protocol. The aim of the thesis was to describe this vulnerability and found out, if it was possible to eliminate it by using different CRC code. It managed to characterize all messages, which are not during this vulnerability detected by CRC code and based on that it was possible to prove, that the probability of error does not depend on a CRC code choice of a fixed length.