CLAIMS

1. A method (200) for securing communications in the V2X standard, in its SAE J2735:2020-07 version, between a transmitting device (2) and a receiving device (3) of an automated driving system (1), characterized in that the method comprises:

- a step (100) of temporally synchronizing a vital computer (24) of the transmitting device (2) and a vital computer (34) of the receiving device, on the basis of least one common external time source (11);
- a step (220) of generating a message in the V2X standard by means of the transmitting device (2), consisting of timestamping the message by requesting a current time from the vital computer (24) of the transmitting device and incorporating the current time as the message timestamp in a field of the message in the V2X standard;
- a step (230) of transmitting the message in the V2X standard, by the transmitting device (2);
- a step (240) of receiving the message in the V2X standard, by the receiving device (3); and
- a step (260) of verifying the temporal validity of the message in the V2X standard, received by the receiving device, by comparing a current time provided by the vital computer of the receiving device with the transmission time incorporated into the received message in the V2X standard,

wherein the step (100) of temporally synchronizing the vital computers (24, 34) of the transmitting and receiving devices uses at least a second external time source, referred to as an auxiliary external time source, which may be different for the transmitting and receiving devices, the temporal synchronization of the vital computer of the transmitting device and the vital computer of the receiving device consisting in:

- initiating (110) the execution of a time server (43, 53) by means of the vital computer;
- sending (130a) a request to the common external time source and receiving (140a) a response containing a first time;
- sending (130b) a request to the auxiliary external time source and receiving (140b) a response containing a second time;
- verifying (155) the consistency between the first and second times, and, if inconsistent, repeating the preceding steps, and, if consistent, establishing an internal time reference which is considered to be a common time base for all components of the system; and
- maintaining (160) the internal time reference.

2. The method according to claim 1, wherein the step (220) of generating a message in the V2X standard further comprises calculating an authentication code, by means of the transmitting device (3), based on the fields of the message in the V2X standard, and a step of incorporating the calculated authentication code into a field of the message, and wherein the method comprises a step (260) of verifying the integrity of the message in the V2X standard, received by the receiving device, by calculating an expected authentication code on the basis of the fields of the received message in the V2X standard and comparing the expected authentication code with the authentication code that is present in the received message in the V2X standard.

3. The method according to claim 2, wherein the authentication code is calculated based on various fields of the message in the V2X standard, by using a hashing algorithm, preferably the SHA-256 algorithm with a dynamic secret hash key known to the various devices of the automated driving system.

4. The method according to claim 2 or claim 3, wherein the authentication code is incorporated into the optional field or a proprietary extension field of the V2X standard.

5. A communication device compatible with the V2X standard, in its SAE J2735:2020-07 version, characterized in that it comprises a vital computer (24, 34) and a radio communication module, the device being configured to implement the steps on the transmitting device side and/or the steps on the receiving device side of the method according to any one of the preceding claims.

6. The communication device according to claim 5, wherein the vital computer is a vital platform of the "2oo2" type.

7. The communication device according to claim 6, wherein the vital platform is capable of guaranteeing a high level of safety in compliance with safety integrity level SIL 4 or ASIL D.