It is therefore necessary to have a person on board the vehicle to take control in case of danger. This standby attendant may be a driver who monitors the vehicle's progress without touching the steering wheel but ready to do so when danger arises.

Summary

The invention therefore aims to solve this problem by proposing communication devices that allow ensuring the safety level of V2X communications between the devices of an autonomous driving system.

To this end, the disclosure relates in an example to a method for securing communications in the V2X standard between a transmitting device and a receiving device of an automated driving system, characterized in that the method comprises: a step of temporally synchronizing the vital computers of the transmitting and receiving devices, on the basis of at least one common external time source; a step of generating a message in the V2X standard ("V2X message") by means of the transmitting device, consisting of timestamping the message by requesting a current time from the vital computer of the transmitting device and incorporating the current time as the message timestamp in a field of the V2X message; a step of transmitting the V2X message, by the transmitting device; a step of receiving the V2X message, by the receiving device; and a step of verifying the temporal validity of the V2X message received by the receiving device, by comparing a current time given by the vital computer of the receiving device with the transmission time incorporated in the received V2X message.

According to some particular examples, this method comprises one or more of the following features, individually or in all technically possible combinations:

- the step of temporally synchronizing the vital computers 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 being performed while taking into account the time references provided by the first and second external sources.

- the step of temporally synchronizing a vital computer consists of: initiating the execution of a time server by means of the vital computer; sending a request to the common external time source and receiving a response containing a first time; sending a request to the auxiliary external time source and receiving a response containing a second time; verifying 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 the internal time reference.

- the step of generating a V2X message further comprises calculating an authentication code, by means of the transmitting device, based on the fields of the V2X message, and a step of incorporating the calculated authentication code into a field of the message, and the method comprises a step of verifying the integrity of the V2X message received by the receiving device by calculating an expected authentication code on the basis of the fields of the received V2X message and comparing the expected authentication code with the authentication code that is present in the received V2X message.

- an authentication code is calculated based on various fields of the V2X message, 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.

- the authentication code is incorporated into the optional field or a proprietary extension field of the V2X standard.

The disclosure also relates in an example to a communication device compatible with the V2X standard, characterized in that it comprises a vital computer 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 above method.

Preferably, the vital computer is a vital platform of the "2oo2" type.

Even more preferably, the vital platform is capable of guaranteeing a high level of safety, complying with safety integrity level SIL 4 or ASIL D.

The disclosure also relates in an example to a communication protocol compatible with the V2X standard, in which each V2X message includes a field incorporating a message timestamp for the V2X message and optionally a field incorporating an authentication code for the V2X message.

In an aspect, the present disclosure refers to 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.

In an aspect, the present disclosure refers to 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 the above aspect.

The invention and its advantages will be better understood by reading the following detailed description of one particular embodiment, given solely as an illustrative and non-

limiting example, this description being made with reference to the appended drawings, in which:

[Fig 1] FIG. 1 is a schematic representation of one embodiment of an automated driving system according to the invention;

[Fig 2] FIG. 2 is a timing diagram of the synchronization process for an internal time source such as the one in FIG. 2; and,

[Fig 3] FIG. 3 is a block diagram representation of the method for securing communications according to the invention, implemented in the system of FIG. 1; and,

[Fig 4] FIG. 4 is a representation of the structure of a V2X message as modified according to the present invention.