(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 109843653 B
(45)授权公告日 2023.05.26

(21)申请号 201880003962.9
(22)申请日 2018.07.19
(65)同一申请的已公布的文献号
申请公布号 CN 109843653 A
(43)申请公布日 2019.06.04
(30)优先权数据
2017-144490 2017.07.26 JP
2018-097207 2018.05.21 JP
(85)PCT国际申请进入国家阶段日
2019.04.18
(86)PCT国际申请的申请数据
PCT/JP2018/027012 2018.07.19
(87)PCT国际申请的公布数据
WO2019/021922 JA 2019.01.31

(73)专利权人 松下电器(美国)知识产权公司
地址 美国加利福尼亚州
(72)发明人 芳贺智之 田边正人 鸟崎唯之 寺泽弘泰 加藤辽
(74)专利代理机构 北京市中咨律师事务所 11247
专利代理师 张洁 段承恩

(51)Int.Cl.
B60R 16/023(2006.01)
B60R 16/02(2006.01)
H04L 12/28(2006.01)

审查员 刘晓鸣

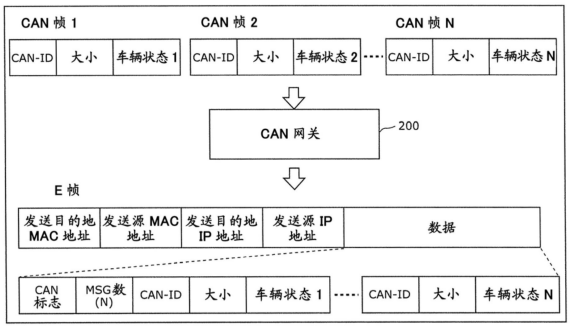
权利要求书2页 说明书18页 附图17页

(54)发明名称

异常检测装置以及异常检测方法

(57)摘要

提供在搭载于移动体的网络系统中检测异常的异常检测装置。异常检测装置检测具有通信协议互不相同的第1网络和第2网络的网络系统中的异常。异常检测装置接收从第2网络取得的表示移动体的状态的状态信息,收发根据第1网络的通信协议的E帧,保持异常检测规则,参照状态信息和异常检测规则来检测接收到的E帧所包含的控制指令是否异常。异常检测装置在检测到控制指令异常的情况下禁止该控制指令的转发。



CN 109843653 B

1.一种异常检测装置,其检测移动体所搭载的网络系统中的异常,所述网络系统具有通信协议互不相同的第1网络和第2网络,所述异常检测装置具备:

第1通信部,其接收从所述第2网络取得的表示所述移动体的状态的状态信息;

第2通信部,其收发根据所述第1网络的通信协议的第1帧;

异常检测规则保持部,其保持异常检测规则;以及

异常检测处理部,其参照所述状态信息和所述异常检测规则,检测在所述第2通信部中接收到的所述第1帧所包含的控制指令是否异常,

所述异常检测处理部在检测到所述控制指令异常的情况下禁止该控制指令的转发,

所述异常检测规则包含表示在所述移动体的不同的多个状态的每个状态下所允许的控制指令的第1规则,

所述异常检测处理部在所述状态信息所示的所述移动体的状态不包含于所述控制指令在所述第1规则中相关联的状态的情况下,检测为所述控制指令异常。

2.根据权利要求1所述的异常检测装置,

所述控制指令是使所述移动体执行前行、转弯和停止中的至少一个的控制指令。

3.根据权利要求1所述的异常检测装置,

所述第1网络是Ethernet即以太网的网络,

所述第2网络是CAN即控制器局域网的网络,

所述第1通信部通过接收包含所述状态信息的CAN帧来接收所述状态信息,

所述异常检测规则还包含用于检测所述CAN帧是否异常的第2规则,

所述异常检测处理部进而在检测到所述CAN帧异常的情况下禁止所述控制指令的转发。

4.根据权利要求1所述的异常检测装置,

所述第1网络是Ethernet即以太网的网络,

所述第2网络是CAN即控制器局域网的网络,

所述第1通信部接收第2帧,所述第2帧是保存有表示所述状态信息的CAN帧的Ethernet帧。

5.根据权利要求4所述的异常检测装置,

所述第2帧保存有包括表示所述状态信息的CAN帧的多个CAN帧,

所述异常检测规则还包含用于检测所述多个CAN帧的每一个是否异常的第2规则,

所述多个CAN帧的每一个具有按种类而不同的标识符,

所述第2规则表示在与多个所述标识符的每一个对应的CAN帧中所允许的CAN帧的接收周期的范围,

所述异常检测处理部使用分别与所述多个CAN帧对应的接收时刻,在彼此具有相同的标识符的所述多个CAN帧之中,在第1CAN帧的第1接收时刻与比所述第1CAN帧早一帧接收到的第2CAN帧的第2接收时刻的差量处于在所述第2规则中与所述相同的标识符相关联的接收周期的范围外的情况下,检测为所述第1CAN帧异常。

6.根据权利要求5所述的异常检测装置,

所述第2规则还表示在与多个所述标识符的每一个对应的CAN帧中所允许的变化量,所述变化量是从该CAN帧的前一个CAN帧的数据值起的变化量,

所述异常检测处理部进而在所述第1CAN帧的第1数据值和所述第2CAN帧的第2数据值的差量超过在所述第2规则中与所述相同的标识符相关联的所述变化量的情况下，检测为所述第1CAN帧异常。

7.根据权利要求4所述的异常检测装置，

所述第2帧保存有包括表示所述状态信息的CAN帧的多个CAN帧，

所述异常检测规则还包含用于检测所述多个CAN帧的每一个是否异常的第3规则，

所述多个CAN帧的每一个具有按种类而不同的标识符，

所述第3规则表示在与多个所述标识符的每一个对应的CAN帧中所允许的CAN帧的接收周期的范围，

所述异常检测处理部使用分别与所述多个CAN帧对应的接收时刻，在彼此具有相同的标识符的所述多个CAN帧之中，在第1CAN帧的第1接收时刻与比所述第1CAN帧早一帧接收到的第2CAN帧的第2接收时刻的差量处于在所述第3规则中与所述相同的标识符相关联的接收周期的范围内的情况下，检测为所述第1CAN帧异常。

8.根据权利要求7所述的异常检测装置，

所述第3规则还表示在与多个所述标识符的每一个对应的CAN帧中所允许的变化量，所述变化量是从该CAN帧的前一个CAN帧的数据值起的变化量，

所述异常检测处理部进而在所述第1CAN帧的第1数据值和所述第2CAN帧的第2数据值的差量处于在所述第3规则中与所述相同的标识符相关联的所述变化量的范围内的情况下，检测为所述第1CAN帧异常。

9.根据权利要求5至8中任一项所述的异常检测装置，

所述异常检测处理部，

取得与多个所述标识符的每一个相关联的规则作为所述异常检测规则，

参照所述异常检测规则来检测所述CAN帧异常。

10.一种异常检测方法，是异常检测装置的异常检测方法，所述异常检测装置检测移动体所搭载的网络系统中的异常，所述网络系统具有通信协议互不相同的第1网络和第2网络，所述异常检测方法包括：

第1通信步骤，接收从所述第2网络取得的表示所述移动体的状态的状态信息；

第2通信步骤，收发根据所述第1网络的通信协议的第1帧；

检测步骤，参照所述状态信息和所述异常检测装置所具备的保持部保持的异常检测规则，检测在所述第2通信步骤中接收到的所述第1帧所包含的控制指令是否异常；

禁止步骤，当在所述检测步骤中检测到所述控制指令异常的情况下，禁止该控制指令的转发，

所述异常检测规则包含表示在所述移动体的不同的多个状态的每个状态下所允许的控制指令的第1规则，

所述检测步骤中，在所述状态信息所示的所述移动体的状态不包含于所述控制指令在所述第1规则中相关联的状态的情况下，检测为所述控制指令异常。

异常检测装置以及异常检测方法

技术领域

[0001] 本公开涉及对搭载于移动体的网络系统中的异常进行检测的异常检测装置以及异常检测方法。

背景技术

[0002] 专利文献1中公开了用于控制车辆的车内网络系统。

[0003] 现有技术文献

[0004] 专利文献1:日本特开2012-6446号公报

发明内容

[0005] 发明所要解决的问题

[0006] 在专利文献1的技术中,有可能无法在如车辆这样的移动体所搭载的网络系统中有效地检测异常。

[0007] 本公开的目的在于,提供能够在移动体所搭载的网络系统中有效地检测异常的异常检测装置以及异常检测方法。

[0008] 用于解决问题的技术方案

[0009] 为了解决上述问题,本公开的一个技术方案涉及的异常检测装置,其检测移动体所搭载的网络系统中的异常,所述网络系统具有通信协议互不相同的第1网络和第2网络,所述异常检测装置具备:第1通信部,其接收从所述第2网络取得的表示所述移动体的状态的状态信息;第2通信部,其收发(接收和发送)根据所述第1网络的通信协议的第1帧(frame);异常检测规则保持部,其保持异常检测规则;以及异常检测处理部,其参照所述状态信息和所述异常检测规则,检测在所述第2通信部中接收到的所述第1帧所包含的控制指令(command,命令)是否异常,所述异常检测处理部在检测到所述控制指令异常的情况下禁止该控制指令的转发。

[0010] 此外,这些总括性的或者具体的技术方案可以通过系统、方法、集成电路、计算机程序或者计算机可读取的CD-ROM等记录介质来实现,也可以通过系统、方法、集成电路、计算机程序以及记录介质的任意组合来实现。

[0011] 发明效果

[0012] 根据本公开的异常检测装置以及异常检测方法,能够在移动体所搭载的网络系统中有效地检测异常。

附图说明

[0013] 图1是实施方式1中的车载网络的整体结构图。

[0014] 图2是表示第2网络中所收发的数据帧(CAN帧)的格式(format)的图。

[0015] 图3是表示第1网络中所收发的E帧的格式的图。

[0016] 图4是表示E帧的有效载荷(payload)内的数据结构例的图。

[0017] 图5是表示CAN网关的功能结构的一例的框图。

[0018] 图6是表示实施方式1涉及的CAN网关基于接收到的多个CAN帧来发送E帧的样子(image)的图。

[0019] 图7是表示自动驾驶DCU的功能结构的一例的框图。

[0020] 图8是表示交换规则保持部所保持的交换规则(switch rule)的一例的图。

[0021] 图9是表示实施方式1涉及的自动驾驶DCU的异常检测规则保持部所保持的异常检测规则的一例的图。

[0022] 图10是表示实施方式1涉及的网络系统中的异常检测方法的一例的时序图。

[0023] 图11是表示实施方式1涉及的网络系统中的异常检测方法的一例的时序图。

[0024] 图12是表示实施方式2涉及的CAN网关基于接收到的多个CAN帧来发送E帧的样子的图。

[0025] 图13是表示实施方式2涉及的自动驾驶DCU的异常检测规则保持部105所保持的异常检测规则的一例的图。

[0026] 图14是表示实施方式2涉及的网络系统中的异常检测方法的一例的时序图。

[0027] 图15是表示实施方式2涉及的网络系统中的异常检测方法的一例的时序图。

[0028] 图16是表示实施方式3涉及的CAN网关基于接收到的多个CAN帧来发送E帧的样子的图。

[0029] 图17是表示实施方式3的自动驾驶DCU中的定义了进行CAN的异常检测时的检测规则的表的图。

具体实施方式

[0030] (成为本发明的基础的见解)

[0031] 关于在“背景技术”中记载的车内网络系统,本发明的发明人发现会产生以下的问题。

[0032] 近年来,在汽车中的系统内,配置有许多被称为电子控制单元(ECU:Electronic Control Unit)的装置。连接这些ECU的网络被称为车载网络。车载网络存在许多标准。在其中最为主流的车载网络之一,存在由ISO11898-1规定的CAN(Controller Area Network:控制器局域网络)这一标准。另外,作为用于传输更多信息的标准,存在由IEEE802.3规定的Ethernet(注册商标,以太网)这一标准。

[0033] 在先进驾驶辅助系统和/或自动驾驶中,需要处理如通过摄像头(camera)或LIDAR(Light Detection and Ranging:激光雷达)等传感器得到的数据、或者动态地图(dynamic map)中使用的数据这样的庞大的量的信息,因而正在引入数据传输速度高的Ethernet(注册商标)。另一方面,现有的CAN也被作为车辆控制系统加以利用。因此,CAN和Ethernet(注册商标)混在一起的车载网络体系结构在增多。

[0034] 将汽车与外部网络连接,逐渐推进汽车的电子控制化。由此,汽车存在由于汽车的控制系统指令被篡改而被不正常操作的威胁。为了保护其不受那样的威胁,在专利文献1的技术中,在从后来安装的电子控制装置对车内网络系统的车辆控制系统网络发送数据的情况下,进行了能否将发送到车内网络的信息系统网络的数据向车辆控制系统网络转发的判断。然而,在专利文献1的技术中,没有依据遵从于多个不同的通信协议而流通的信息进行

能否转发的判断。因此，在现有技术中，例如存在如下问题：当在根据如CAN以及Ethernet(注册商标)这样的互不相同的通信协议的多个网络之间进行数据的转发的情况下，无法适当地进行能否转发的判断。

[0035] 本发明人在认真研究之后，发现了通过参照遵从于多个不同的通信协议而流通的信息并判断车辆控制系统的消息是否不正常从而用于实现安全的自动驾驶或先进驾驶辅助系统的异常检测装置以及异常检测方法。

[0036] 本公开的一个技术方案涉及的异常检测装置，其检测移动体所搭载的网络系统中的异常，所述网络系统具有通信协议互不相同的第1网络和第2网络，所述异常检测装置具备：第1通信部，其接收从所述第2网络取得的表示所述移动体的状态的状态信息；第2通信部，其收发根据所述第1网络的通信协议的第1帧；异常检测规则保持部，其保持异常检测规则；以及异常检测处理部，其参照所述状态信息和所述异常检测规则，检测在所述第2通信部中接收到的所述第1帧所包含的控制指令是否异常，所述异常检测处理部在检测到所述控制指令异常的情况下禁止该控制指令的转发。

[0037] 由此，异常检测装置基于异常检测规则和从第2网络获得的移动体的状态信息，检测被生成的自动驾驶的控制指令是否异常。因此，能够在移动体所搭载的网络系统中有效地检测异常。

[0038] 另外，异常检测装置禁止对检测出有异常的控制指令的转发。因此，例如即使在连接于第1网络的设备有脆弱性并经由第1网络受到攻击的情况下，异常检测装置也能够防止不正常的自动驾驶控制。能够在异常检测时防止诸如自动驾驶和/或先进驾驶系统之类的车辆控制指令的执行。

[0039] 另外，也可以为，所述异常检测规则包含表示在所述移动体的不同的多个状态的每个状态下所允许的控制指令的第1规则，所述异常检测处理部在所述状态信息所示的所述移动体的状态不包含于所述控制指令在所述第1规则中相关联的状态的情况下，检测为所述控制指令异常。

[0040] 由此，异常检测装置例如能够基于目前的车速、转向器(steering)的操舵角度状态、挡位(shift position)等车辆状态来检测车辆控制指令的异常。

[0041] 另外，也可以为，所述控制指令是使所述移动体执行前行、转弯和停止中的至少一个的控制指令。

[0042] 由此，异常检测装置例如能够检测行驶中的急转弯、急刹车和/或急加速、停车中的急起动等、自动驾驶或者先进驾驶辅助系统的控制指令的异常，提供安全的驾驶环境。

[0043] 另外，也可以为，所述第1网络是Ethernet(注册商标)的网络，所述第2网络是CAN的网络，所述第1通信部通过接收包含所述状态信息的CAN帧来接收所述状态信息，所述异常检测规则还包含用于检测所述CAN帧是否异常的第2规则，所述异常检测处理部进而在检测到所述CAN帧异常的情况下禁止所述控制指令的转发。

[0044] 由此，能够在检测了CAN帧的异常之后进行车辆控制指令的执行。

[0045] 另外，也可以为，所述第1网络是Ethernet(注册商标)的网络，所述第2网络是CAN的网络，所述第1通信部接收作为保存有表示所述状态信息的CAN帧的Ethernet(注册商标)帧的第2帧。

[0046] 由此，能够使得表示状态信息的CAN帧保存于Ethernet(注册商标)帧，通过

Ethernet(注册商标)上的设备进行CAN帧的异常检测。

[0047] 另外,也可以为,所述第2帧保存有包括表示所述状态信息的CAN帧的多个CAN帧,所述异常检测规则还包含用于检测所述多个CAN帧的每一个是否异常的第2规则,所述多个CAN帧的每一个具有按种类而不同的标识符,所述第2规则表示在与多个所述标识符的每一个对应的CAN帧中所允许的CAN帧的接收周期的范围,所述异常检测处理部使用分别与所述多个CAN帧对应的接收时刻,在彼此具有相同的标识符的所述多个CAN帧之中,在第1CAN帧的第1接收时刻与比所述第1CAN帧早一帧接收到的第2CAN帧的第2接收时刻的差量处于在所述第2规则中与所述相同的标识符相关联的接收周期的范围外的情况下,检测为所述第1CAN帧异常。

[0048] 由此,即使是在第2网络上发生了异常的情况下,也能够在第1网络中的设备中检测具有周期性的CAN帧的异常,因此能够安全地使自动驾驶和/或先进驾驶辅助系统停止。

[0049] 另外,也可以为,所述第2规则还表示在与多个所述标识符的每一个对应的状态信息中所允许的变化量,所述变化量是从该状态信息的前一个状态信息的数据值起的变化量,所述异常检测处理部进而在所述第1状态信息的第1数据值和所述第2状态信息的第2数据的差量超过在所述第2规则中与所述相同的标识符相关联的所述变化量的情况下,检测为所述第1状态信息异常。

[0050] 由此,利用异常检测装置,即使是在第2网络上发生了异常的情况下,也能够在第1网络中的设备中检测CAN帧的数据值的异常,因此能够停止自动驾驶。

[0051] 另外,也可以为,所述第2帧保存有包括表示所述状态信息的CAN帧的多个CAN帧,所述异常检测规则还包含用于检测所述多个CAN帧的每一个是否异常的第3规则,所述多个CAN帧的每一个具有按种类而不同的标识符,所述第3规则表示在与多个所述标识符的每一个对应的CAN帧中所允许的CAN帧的接收周期的范围,所述异常检测处理部使用分别与所述多个CAN帧对应的接收时刻,在彼此具有相同的标识符的所述多个CAN帧之中,在第1CAN帧的第1接收时刻与比所述第1CAN帧早一帧接收到的第2CAN帧的第2接收时刻的差量处于在所述第3规则中与所述相同的标识符相关联的接收周期的范围内的情况下,检测为所述第1CAN帧异常。

[0052] 由此,即使是在第2网络上发生了异常的情况下,也能够在第1网络中的设备中检测具有周期性的CAN帧的异常,因此能够安全地使自动驾驶和/或先进驾驶辅助系统停止。

[0053] 另外,也可以为,所述第3规则还表示在与多个所述标识符的每一个对应的CAN帧中所允许的变化量,所述变化量是从该CAN帧的前一个CAN帧的数据值起的变化量,所述异常检测处理部进而在所述第1CAN帧的第1数据值和所述第2CAN帧的第2数据值的差量处于在所述第3规则中与所述相同的标识符相关联的所述变化量的范围内的情况下,检测为所述第1CAN帧异常。

[0054] 由此,利用异常检测装置,即使是在第2网络上发生了异常的情况下,也能够在第1网络中的设备中检测CAN帧的数据值的异常,因此能够停止自动驾驶。

[0055] 另外,也可以为,所述异常检测处理部取得与多个所述标识符的每一个相关联的规则作为所述异常检测规则,参照所述异常检测规则来检测所述状态信息异常。

[0056] 由此,例如能够在第2网络侧的处理紧迫时,通过第1网络上的设备实施第2网络上的异常检测,分散负荷。

[0057] 此外，这些总括性的或者具体的技术方案可以通过系统、方法、集成电路、计算机程序或者能够由计算机读取的CD-ROM等记录介质来实现，也可以通过系统、方法、集成电路、计算机程序以及记录介质的任意组合来实现。

[0058] 以下，参照附图，对实施方式涉及的异常检测装置以及异常检测方法进行说明。在此所示的实施方式都是表示本公开的一个具体例子的实施方式。因此，在以下的实施方式中表示的数值、构成要素、构成要素的配置和连接方式、以及作为处理的要素的步骤和步骤的顺序等仅为一例而不限定本公开。对于以下的实施方式中的构成要素中的、没有记载在独立权利要求中的构成要素，是可以任意附加的构成要素。另外，各附图为示意图，不一定是严格图示。

[0059] (实施方式1)

[0060] 图1是实施方式1中的车载网络的整体结构图。

[0061] 车辆1的网络系统3是搭载有控制装置、传感器、致动器、用户接口装置等各种设备的车辆1中的网络通信系统。网络系统3具有第1网络10和第2网络20。车辆1是移动体的一例。第1网络10是遵循Ethernet(注册商标)协议进行Ethernet(注册商标)帧(以下称为“E帧”)的传输的Ethernet(注册商标)网络。第2网络20是遵循CAN协议通过总线进行数据帧(CAN帧)等的传输的CAN网络。

[0062] 如图1所示，网络系统3构成为包括中央网关400、远程信息控制单元(Telematics Control Unit)410、诊断端口420、自动驾驶DCU(Domain Control Unit)100、自动驾驶ECU110、摄像头120、LIDAR130、动态地图ECU140、信息娱乐DCU300、IVI(In-Vehicle Infotainment:车载信息娱乐系统)310、CAN网关200、发动机ECU210、转向器ECU220、制动器ECU230、车窗ECU240、第1传输线路11和第2传输线路21。第1传输线路11是第1网络10的传输线路，例如是Ethernet(注册商标)电缆。第2传输线路21是第2网络20的传输线路，例如是CAN总线。

[0063] 此外，在网络系统3中，除了上述的各ECU110、140、210、220、230、240或各DCU100、300之外，可以还包括若干个ECU或DCU。例如，在第2传输线路21上，除了各ECU210、220、230、240以外，也可以连接有未图示的ECU。

[0064] 各ECU110、140、210、220、230、240或各DCU100、300例如是包括处理器(微处理器)、存储器等的数字电路、模拟电路、通信电路等的装置。存储器是ROM、RAM等，能够存储由处理器执行的程序(作为软件的计算机程序)。作为存储器，也可以包括非易失性存储器。例如处理器按照程序(计算机程序)进行工作，由此ECU会实现各种功能。此外，计算机程序是为了实现预定功能而组合多个表示对处理器的指令的命令码而构成的。

[0065] 各ECU210、220、230、240遵循CAN协议进行帧的授受。各ECU210、220、230、240分别连接于诸如发动机、转向器、制动器、车窗开闭传感器之类的设备，取得该设备的状态，例如周期性地将表示状态的数据帧发送到通过第2传输线路21等构成的第2网络20。另外，各ECU210、220、230、240从构成第2网络20的第2传输线路21接收数据帧，解释数据帧并进行数据帧是否具有应该接收的CAN-ID的判别。而且，判别的结果，各ECU210、220、230、240既可以根据需要按照数据帧内的数据(数据域的内容)进行连接于该ECU的设备的控制，也可以根据需要生成并发送数据帧。

[0066] 各ECU110、140或各DCU100、300遵循Ethernet(注册商标)协议进行E帧的发送或接

收。各DCU100、300分别连接于诸如IVI310、自动驾驶ECU110、摄像头120、LIDAR130、动态地图ECU140之类的设备，进行基于从该设备取得的信息的处理。另外，各DCU100、300既可以根据需要控制所连接的设备，也可以根据需要进行向其他ECU发送信息。

[0067] 对于中央网关400，通过第1传输线路11连接有远程信息控制单元410和诊断端口420、自动驾驶DCU100、CAN网关200、以及信息娱乐DCU300。中央网关400例如包括存储器等的数字电路、模拟电路、通信电路等。

[0068] 远程信息控制单元410是车辆1与位于外部网络30上的服务器2进行通信的单元。远程信息控制单元410例如既可以具有适于如第三代移动通信系统(3G)、第四代移动通信系统(4G)或LTE(注册商标)等这样的移动通信系统中所利用的通信标准的无线通信接口，也可以具有适于IEEE802.11a、b、g、n标准的无线局域网(LAN:Local Area Network)接口。也即是说，外部网络30是手机通信网、Wi-Fi等。服务器2例如是具有对车辆1的ECU提供信息的功能等的计算机。

[0069] 诊断端口420是用于经销商(dealer)用以诊断车辆1的故障的端口，是收发诊断用的指令所利用的端口。

[0070] 自动驾驶DCU100通过第1传输线路11与自动驾驶ECU110、摄像头120、LIDAR130和动态地图ECU140相连接。

[0071] 自动驾驶ECU110生成控制车辆1的驾驶的控制指令。具体而言，自动驾驶ECU110生成控制进行车轮的操舵的转向器、使车轮旋转驱动的发动机、马达等驱动源、制动车轮的制动器等的控制指令。也即是说，控制指令是使车辆1执行前行(也即是说行驶)、转弯和停止中的至少一个的控制指令。自动驾驶ECU110将生成的控制指令发送到第2网络20。

[0072] 摄像头120是拍摄车外状况、也即是说车辆1周围的摄像头。摄像头120例如也可以配置在车辆1的车体外侧。

[0073] LIDAR130是用于感测车外的障碍物的传感器。LIDAR130例如是检测与处于车辆1的水平方向上的360度全方位以及垂直方向上的预定角度(例如30度)的角度范围的检测范围内的物体之间的距离的激光传感器。LIDAR130通过对车辆1周围发射激光并检测被周围物体反射的激光，由此计测从LIDAR130到物体的距离。

[0074] 动态地图ECU140是用于接收动态地图所用的数据并使用接收到的数据来解密动态地图的电子控制单元。解密出的动态地图例如被用于自动驾驶ECU110的自动驾驶的控制。

[0075] CAN网关200是连接于第2网络20以及第1网络10的网关。在本实施方式中，第2网络20具备如下两条CAN总线:发动机ECU210、转向器ECU220、制动器ECU230的控制系统总线;控制车窗开闭的车窗ECU240所连接的车身(body)系统总线。CAN网关200包括处理器、存储器等的数字电路、模拟电路、通信电路等。CAN网关200具有将从两条传输线路11、21中的一条传输线路接收到的帧转发(或者中继)到另一条传输线路的功能。由CAN网关200对帧的转发是帧所涉及的数据的中继。CAN网关200也可以在帧的转发中进行与在转发目的地的传输线路上所使用的通信协议对应的通信方式、帧格式等的变换。另外，CAN网关200也可以对应于从一条以上的传输线路接收到的一个以上的帧来进行一个以上的帧的向一条以上的多条传输线路的发送，作为在传输线路间的帧的转发。

[0076] 信息娱乐DCU300通过第1传输线路11与IVI310相连接，进行信息系统网络的域管

理。IVI310具备显示器，是具有诸如影像、声音等的再现之类的多媒体功能的装置。

[0077] 图2是表示第2网络中所收发的数据帧(CAN帧)的格式的图。

[0078] 在第2网络20中，各ECU210、220、230、240等遵循CAN协议进行帧的授受。CAN协议中的帧有数据帧、远程帧、过载帧以及错误帧，但这里主要关注数据帧来进行说明。

[0079] 图2的(a)是标准格式。在标准格式中，数据帧由SOF(Start Of Frame:帧起始)、ID(CAN-ID)、RTR(Remote Transmission Request:远程传输请求)、IDE(Identifier Extension:标识符扩展)、预留位“r”、大小(size)、数据、CRC(Cyclic Redundancy Check:循环冗余校验)序列、CRC定界符“DEL”、ACK(Acknowledgement:应答)间隙(slot)、ACK定界符“DEL”以及EOF(End Of Frame:帧结束)构成。在此，作为ID域的内容的ID(CAN-ID)是表示数据种类的标识符，也被称为消息ID。也即是说，CAN帧按每个种类具有不同的标识符。此外，关于CAN，在多个节点同时开始发送的情况下，做出使该CAN-ID具有小值的帧优先的通信仲裁(调停)。大小是表示后续的数据域(数据)的长度的DLC(Data Length Code)。关于数据(数据域的内容)的规格，没有在CAN协议中规定，而在网络系统3中确定。因此，能够成为取决于车辆的车型、制造者(制造商)等的规格。

[0080] 图2的(b)是扩展格式。在本实施方式中设为在第2网络20中使用了标准格式来进行说明，而在第1网络10中使用扩展格式的情况下，只要将使11比特(位)的ID域的基础ID(CAN-ID的一部分)和18比特的扩展ID(CAN-ID的剩余部分)合在一起的29比特视为CAN-ID即可。

[0081] 图3是表示第1网络中所收发的E帧的格式的图。

[0082] 如该图所示，E帧由保存作为主要传输内容的数据的Ethernet(注册商标)有效载荷(也称为“E有效载荷”。)和Ethernet(注册商标)头(也称为“E头”。)构成。E头中包含接收方MAC地址以及发送源MAC地址。另外，E有效载荷中包含IP头、TCP/UDP头以及数据。IP头中包含发送源IP地址以及发送目的地IP地址。此外，在图3中，IP头表示为“IPv4头”。TCP/UDP头表示TCP头或者UDP头，TCP/UDP头中包含发送源端口号以及发送目的地端口号。

[0083] 网络系统3中的CAN网关200在将从CAN总线接收到的CAN帧向第1网络10转发时发送包含多个CAN帧信息的E帧。CAN帧信息是从通过CAN总线传输来的CAN帧中提取到的信息，至少包含数据域的内容(数据)。CAN帧信息例如也可以包含CAN-ID以及大小。

[0084] 将图3所示的E帧的有效载荷内的数据结构例表示于图4。在图4的例子中，CAN帧信息由CAN-ID、大小以及数据构成。图4的消息数(MSG数)表示CAN帧信息的个数。此外，也可以取代消息数而使用表示CAN帧信息整体的数据量等的信息。另外，CAN标志是用于识别E帧是否包含从第2网络20传输的信息(也即是说CAN帧信息)的识别标志，是当在E帧的E有效载荷中包含CAN帧信息的情况下设为ON(是)、否则设为OFF(否)(也即是说表示与ON相反的信息的值)的标志。在图4的例子中，表示了在E帧的E有效载荷的最前头配置CAN标志的例子，但这不过是一例。通过如图4的例子这样使多个CAN帧信息包含于E帧的E有效载荷，例如传输效率能够提高。

[0085] 图5是表示CAN网关的功能结构的一例的框图。

[0086] 如该图所示，CAN网关200具备Ethernet(注册商标)收发部201(以下称为“E收发部201”。)、CAN收发部202a、202b、转发控制部203、以及转发规则保持部204。这些各构成要素由CAN网关200中的通信电路、存储器、数字电路、执行存储器所保存的程序的处理器等来实

现。

[0087] E收发部201是连接于构成第1网络10的第1传输线路11的通信电路等。E收发部201从第1传输线路11接收E帧。另外，E收发部201向第1传输线路11发送E帧。

[0088] CAN收发部202a是连接于构成第2网络20的CAN总线21a的通信电路等。CAN收发部202a从CAN总线21a逐次接收CAN帧。另外，CAN收发部202a向CAN总线21a发送CAN帧。

[0089] CAN收发部202b是连接于构成第2网络20的CAN总线21b的通信电路等。CAN收发部202b从CAN总线21b逐次接收CAN帧。CAN收发部202b向CAN总线21b发送CAN帧。

[0090] 转发规则保持部204通过存储器等存储介质实现，保持确定帧转发的条件等的基准信息。基准信息例如是使转发对象的CAN-ID以及转发源的总线与接收方(MAC地址等)相关联的转发规则信息、使优先转发对象的CAN-ID以及转发源的总线与接收方相关联的优先转发列表等。

[0091] 转发控制部203例如通过执行程序的处理器等实现，判定是否应该转发接收到的帧并根据判定结果进行转发所涉及的控制。该转发所涉及的控制例如是如下控制：使E收发部201基于逐次接收到的多个CAN帧，将含有多个CAN帧信息作为有效载荷的E帧向第1传输线路11进行发送。

[0092] 图6是表示实施方式1涉及的CAN网关200基于接收到的多个CAN帧(CAN帧1～N)来发送E帧的样子的图。

[0093] 如该图所示，CAN网关200在转发帧时，变更帧的结构。被发送的E帧的有效载荷中例如包含作为预先确定的数量的N个CAN帧信息。该N个CAN帧信息的数据是所接收到的N个CAN帧的数据域的内容(数据)等。被接收并等待转发的CAN帧的内容例如保存于CAN网关200所具备的存储器等存储介质(缓冲器)。图6的包含N个CAN帧信息的E帧例如将会经由中央网关400而被接收方的ECU或者DCU(例如信息娱乐DCU300)接收。作为E帧的头的发送源MAC地址，设定有CAN网关200的MAC地址，在E帧的E有效载荷中设定有表示包含CAN帧信息这一情况的设为ON的CAN标志。作为E帧的接收方MAC地址，按照转发规则保持部204保持的转发规则信息等，设定有成为接收方的ECU或者DCU的MAC地址。

[0094] 此外，在本实施方式中，CAN网关200为了检测自动驾驶的控制指令的异常，将流通于第2网络20的包含表示车辆状态的状态信息的N个CAN帧结合从而变换成一个E帧。在本实施方式中，CAN帧所包含的车辆状态是当前的车速、转向器的角度、挡位等。车辆状态是移动体的状态的一例。

[0095] 转发控制部203根据判定等的结果来在一定条件下控制E收发部201、CAN收发部202a、202b，使之进行帧的发送。对于由CAN收发部202a、202b接收到的CAN帧，转发控制部203基于CAN-ID来判定该CAN帧的数据是否应该被发送到第1网络10。该判定例如按照预先确定的与CAN-ID有关的基准信息来进行。另外，转发控制部203按照基准信息来选定CAN帧的数据的接收方。CAN帧是否应该被发送到第1网络10的判定以及包含CAN帧的数据的帧(E帧或CAN帧)的接收方的选定例如使用转发规则信息来进行，所述转发规则信息表示数据应该被发送到第1网络10的一个以上的CAN帧的CAN-ID等。

[0096] 图7是表示自动驾驶DCU100的功能结构的一例的框图。

[0097] 如该图所示，自动驾驶DCU100具有第1通信部101a、第2通信部101b、交换处理部102、交换规则保持部103、异常检测处理部104、以及异常检测规则保持部105。自动驾驶

DCU100是异常检测装置的一例。

[0098] 第1通信部101a在本实施方式中具备一个Ethernet(注册商标)端口(端口P1)。端口P1与中央网关400通过第1传输线路11相连接。也即是说,第1通信部101a在与中央网关400之间进行数据的收发。也即是说,第1通信部101a接收保存有CAN帧作为数据的E帧。由此,第1通信部101a通过接收CAN帧来接收CAN帧所包含的状态信息。

[0099] 第2通信部101b在本实施方式中具备四个Ethernet(注册商标)端口(端口P2～P5)。端口P2～P5分别与摄像头120、LIDAR130、动态地图ECU140以及自动驾驶ECU110通过第1传输线路11相连接。也即是说,第2通信部101b收发根据第1网络10的通信协议(也即是说Ethernet(注册商标)协议)的第1帧(也即是说E帧)。另外,第2通信部101b包括进行在端口P1的E帧的收发的第1通信部101a。

[0100] 交换处理部102进行如下处理:将由第2通信部101b接收到的E帧基于交换规则保持部103所保持的规则转发到适当的转发目的地。

[0101] 图8是表示交换规则保持部103所保持的交换规则的一例的图。

[0102] 如该图所示,交换规则由输入端口、发送源IP地址、发送源MAC地址、输出端口、发送目的地IP地址、发送目的地MAC地址构成。本实施方式中的交换规则是表示正常的E帧的正确的转发目的地的白名单(white list)。在交换规则中,例如表示了允许来自CAN网关200的E帧经由中央网关400而在端口P1被接收并向连接于端口P5的自动驾驶ECU110进行转发的路径。在该情况下,在成为输入端口的端口P1接收的E帧的发送源MAC地址设定成了中央网关400的MAC地址,发送源IP地址设定成了CAN网关200的IP地址。另一方面,成为输出端口的端口P5所连接的发送目的地IP地址以及发送目的地MAC地址中设定有自动驾驶ECU的IP地址以及MAC地址。

[0103] 另外,在图8的交换规则中,表示了允许连接于端口P2的摄像头120、连接于端口P3的LIDAR130以及连接于端口P4的动态地图ECU140向端口P5所连接的自动驾驶ECU110的转发。另外,来自端口P5所连接的自动驾驶ECU110的E帧需要向CAN网关200发送,因此,发送目的地IP地址中设定有CAN网关200的IP地址,发送目的地MAC地址中设定有中央网关的MAC地址。

[0104] 此外,在交换规则中,输入或输出的发送源以及发送目的地由IP地址以及MAC地址进行了定义,但不限定于此。例如,既可以仅定义有IP地址,也可以仅定义有MAC地址。另外,在交换规则中,既可以定义有除IP地址或MAC地址以外的能够识别发送源或发送目的地的信息,也可以定义有服务端口号。由此,能够将输入或输出的发送源以及发送目的地限制于由交换规则所允许的路径。

[0105] 图8的交换规则是由白名单定义的,但也可以由黑名单来定义。另外,图8中示出的交换规则是一部分,并非全部。也即是说,交换规则设定为包罗所需的路径。

[0106] 异常检测处理部104参照由第1通信部101a经由CAN网关200从第2网络20接收到的车辆1的状态信息、和异常检测规则保持部105所保持的异常检测规则,检测在第2通信部101b中接收到的E帧所包含的控制指令是否异常。控制指令例如是自动驾驶ECU110生成的自动驾驶控制指令。异常检测处理部104在判断为控制指令正常的情况下,使第2通信部101b将该控制指令从中央网关400经由CAN网关200向第2网络20发送。异常检测处理部104在判断为控制指令异常的情况下,禁止由第2通信部101b对控制指令的向第2网络20的转

发。

[0107] 图9是表示实施方式1涉及的自动驾驶DCU100的异常检测规则保持部105所保持的异常检测规则的一例的图。异常检测规则是以从第2网络20取得的车辆状态为基础的Ethernet(注册商标)中的自动驾驶控制被允许的规则。也即是说,异常检测规则包含表示在车辆的多个状态的每个状态下所允许的控制指令的第1规则。

[0108] 如该图所示,异常检测规则的第1规则表示根据车辆1的车速状态以及换挡状态所允许的、车速指示和操舵指示的组合。此外,所谓车速状态,表示车辆1的行驶中的速度,例如将0km/h以上且不足30km/h的速度范围、30km/h以上且不足60km/h的速度、和60km/h以上且100km/h以下分别定义为低速、中速和高速。另外,所谓换挡状态,表示挡位,例如为停车挡(P)、倒车挡(R)、空挡(N)、前进挡(D)等。车速指示表示从当前车速起所允许的增减速度值。另外,操舵指示表示从当前的转向器的转动角度起所允许的增减角度。

[0109] 在第1规则中,例如在车速状态为低速、并且换挡状态为前进挡(D)时,如果自动驾驶控制中的车速指示为距状态信息所示的目前的车速在10km/h的范围内,则允许增减车速。另外,在第1规则中,例如在车速状态为中速、并且换挡状态为前进挡(D)时,如果自动驾驶控制中的车速指示为距状态信息所示的目前的车速在20km/h的范围内,则允许增减车速。另外,在第1规则中,例如在车速状态为高速、并且换挡状态为前进挡(D)时,如果自动驾驶控制中的车速指示为距状态信息所示的目前的车速在30km/h的范围内,则允许增减车速。

[0110] 在第1规则中,关于操舵指示的转向器的转动指示角度,也与车速同样进行了定义。也即是说,在第1规则中,例如在车速状态为低速、并且换挡状态为前进挡(D)时,如果自动驾驶控制中的操舵指示为距状态信息所示的目前的转向器的角度在左右360度以内,则允许变更转向器的角度。另外,在第1规则中,例如在车速状态为中速、并且换挡状态为前进挡(D)时,如果自动驾驶控制中的操舵指示为距状态信息所示的目前的转向器的角度在左右180度以内,则允许变更转向器的角度。另外,在第1规则中,例如在车速状态为高速、并且换挡状态为前进挡(D)时,如果自动驾驶控制中的操舵指示为距状态信息所示的目前的转向器的角度在左右90度以内,则允许变更转向器的角度。

[0111] 异常检测处理部104在状态信息所示的车辆1的状态不包含于控制指令在第1规则中相关联的状态的情况下,检测为控制指令异常。也即是说,异常检测处理部104例如在由第2通信部101b接收到包含超过在第1规则中关联于车辆状态的所允许的车速增减的范围的车速指示、或者超过在第1规则中关联于车辆状态的所允许的转向器角度的范围的操舵指示的控制指令的情况下,检测为该控制指令异常,禁止由第1通信部101a向第2网络20进行该控制指令的转发。

[0112] 接着,对实施方式1涉及的车辆1所搭载的网络系统3的工作进行说明。

[0113] 图10以及图11是表示实施方式1涉及的网络系统3中的异常检测方法的一例的时序图。

[0114] 首先,自动驾驶DCU100针对自动驾驶ECU110,使自动驾驶模式成为有效状态(S100)。例如,在受理到来自用户的使自动驾驶模式开启的输入的情况下,自动驾驶DCU100使自动驾驶模式成为有效状态。

[0115] CAN网关200从连接于CAN网关200的各ECU210、220、230、240接收包含车辆1的状态

信息的CAN帧，并如图6所示那样，生成含有车辆1的状态信息的CAN帧的E帧(S101)。

[0116] CAN网关200将包含车辆1的状态信息的CAN帧的E帧发送给中央网关400(S102)。

[0117] 中央网关400将在步骤S102中接收到的E帧发送给自动驾驶DCU100(S103)。

[0118] 在自动驾驶DCU100中，第2通信部101b分别从摄像头120、LIDAR130以及动态地图ECU140接收表示由摄像头120拍摄到的影像的影像信息、基于表示由LIDAR130检测到的到物体的距离的信息的障碍物信息、由动态地图ECU140获得的地图信息(S104)。

[0119] 在自动驾驶DCU100中，交换处理部102参照交换规则保持部103的交换规则，判定是否用正确的路径接收了信息(S105)。

[0120] 由此，在自动驾驶DCU100中，将在步骤S104中第2通信部101b从摄像头120、LIDAR130、动态地图ECU140接收到的影像信息、障碍物信息以及地图信息等信息中的、由交换处理部102判定为是用正确的路径接收的信息转发给自动驾驶ECU110(S106)。

[0121] 自动驾驶ECU110基于在步骤S106中接收到的影像信息、障碍物信息以及地图信息等信息，生成用于自动驾驶的控制指令(S107)。在此，自动驾驶ECU110首先生成用于传达给控制系统CAN总线的CAN帧，并生成将这些CAN帧保存于E帧的数据区域的E帧。所生成的E帧是用于自动驾驶的控制指令。

[0122] 自动驾驶ECU110将用于自动驾驶的控制指令发送给自动驾驶DCU100(S108)。

[0123] 在自动驾驶DCU100中，异常检测处理部104参照异常检测规则保持部105所保持的异常检测规则(S109)。在此参照的规则是图9中示出的第1规则。

[0124] 在自动驾驶DCU100中，异常检测处理部104除了参照异常检测规则之外，还参照在S103中接收到的包含有车辆1的状态信息的CAN帧的E帧，判定第2通信部101b通过步骤S108接收到的控制指令是否异常(S110)。异常检测处理部104在判定为控制指令异常的情况下(步骤S110:异常)，将处理移至步骤S111。另一方面，异常检测处理部104在判定为控制指令正常的情况下(步骤S110:正常)，将处理移至步骤S120。

[0125] 在自动驾驶DCU100中，异常检测处理部104由于判定为控制指令异常因而使用第2通信部101b向服务器2或者IVI310通知包含存在异常这一情况的信息(S111)。由此，驾驶员或者远程进行监视的安全监视服务的操作员能够掌握到车辆1在自动驾驶中发生了异常。此外，在该情况下，异常检测处理部104不将控制指令发送给中央网关400。也即是说，异常检测处理部104在该情况下禁止将判定为异常的控制指令经由中央网关400以及CAN网关200向第2网络20转发。

[0126] 在自动驾驶DCU100中，异常检测处理部104使用第2通信部101b对自动驾驶ECU110发送使其结束自动驾驶的结束指示(S112)。

[0127] 自动驾驶ECU110在接收到在步骤S112中发送来的结束指示的情况下，结束自动驾驶模式(S113)。此外，自动驾驶ECU110也可以在结束自动驾驶模式后切换到手动驾驶模式。

[0128] 在步骤S110中，判定为控制指令正常的情况下(S110:正常)，异常检测处理部104使用第2通信部101b将用于自动驾驶的控制指令发送给中央网关400(S120)。

[0129] 中央网关400将在步骤S120中发送来的自动驾驶控制指令转发给CAN网关200(S121)。

[0130] CAN网关200将通过步骤S121接收到的E帧的自动驾驶的控制指令变换为CAN帧(S122)。

[0131] CAN网关200将通过步骤S122变换出的CAN帧发送到第2网络20(S123)。由此,连接于控制系统CAN总线的发动机ECU210、转向器ECU220或者制动器ECU230接收CAN帧的自动驾驶的控制指令,通过执行与接收到的控制指令相应的控制来进行自动驾驶控制。

[0132] 本实施方式涉及的异常检测装置是检测车辆1所搭载的具有通信协议互不相同的第1网络10和第2网络20的网络系统3中的异常的异常检测装置。自动驾驶DCU100具备第1通信部101a、第2通信部101b、异常检测规则保持部105以及异常检测处理部104。第1通信部101a接收从第2网络20取得的表示车辆1的状态的状态信息。第2通信部101b收发根据第1网络10的通信协议的E帧。异常检测规则保持部105保持异常检测规则。异常检测处理部104参照状态信息和异常检测规则,检测在第2通信部101b中接收到的E帧所包含的控制指令是否异常。异常检测处理部104在检测到控制指令异常的情况下禁止该控制指令的转发。

[0133] 由此,异常检测装置基于异常检测规则和从第2网络20获得的车辆1的状态信息,检测被生成的自动驾驶的控制指令是否异常。而且,异常检测装置禁止对检测出有异常的控制指令的转发。因此,例如即使在连接于第1网络10的设备有脆弱性并经由第1网络10受到攻击的情况下,异常检测装置也能够防止不正常的自动驾驶控制。

[0134] 另外,在本实施方式涉及的异常检测装置中,异常检测规则包含表示在车辆1的不同的多个状态的每个状态下所允许的控制指令的第1规则。异常检测处理部104在状态信息所示的车辆1的状态不包含于控制指令在第1规则中相关联的状态的情况下,检测为控制指令异常。因此,能够例如基于目前的车速、转向器的操舵角度、挡位等车辆状态来检测控制指令的异常。

[0135] 另外,在本实施方式涉及的异常检测装置中,控制指令是使车辆1执行前行、转弯和停止中的至少一个的控制指令。因此,异常检测装置例如能够检测行驶中的急转弯、急刹车或急加速、停车中的急起动等自动驾驶中的控制指令的异常,提供安全的驾驶环境。

[0136] 另外,在本实施方式涉及的异常检测装置中,第1通信部101a接收第1帧,所述第1帧是保存有CAN帧作为数据的E帧。另外,第2通信部101b包括第1通信部101a。由此,异常检测装置接收被变换为E帧的CAN帧,因而能够用Ethernet(注册商标)上的设备进行CAN帧的异常检测。

[0137] (实施方式2)

[0138] 接着对实施方式2进行说明。实施方式2涉及的作为异常检测装置的自动驾驶DCU100与实施方式1涉及的自动驾驶DCU100大致等同,因此仅对不同的部分进行说明。在实施方式2中,与实施方式1涉及的自动驾驶DCU100的不同之处在于,在自动驾驶DCU100中也进行CAN帧的异常检测。

[0139] 图12是表示实施方式2涉及的CAN网关200基于接收到的多个CAN帧来发送E帧的样子的图。

[0140] 在本实施方式中,自动驾驶DCU100确认CAN帧的周期来进行CAN的异常检测。如图12所示,CAN网关200接收多个CAN帧,并针对接收到的多个CAN帧的每一个,对该CAN帧附加接收到该CAN帧的接收时刻。也即是说,CAN网关200通过将N个被附加了接收时刻的CAN帧保存于E帧的数据区域来生成E帧。与实施方式1同样地,CAN网关200封装成E帧的CAN帧所包含的车辆1的状态信息是车速、转向器的角度或挡位等。

[0141] 自动驾驶DCU100的第2通信部101b接收图12的结构的E帧,因而将会接收保存有多

个CAN帧、和多个CAN帧的每一个例如由CAN网关200等设备接收到的时刻即接收时刻作为数据的E帧。

[0142] 图13是表示实施方式2涉及的自动驾驶DCU100的异常检测规则保持部105所保持的异常检测规则的一例的图。图13所示的异常检测规则是用于检测CAN帧是否异常的第2规则的一例。

[0143] 如该图所示，第2规则表示在与CAN-ID对应的CAN帧中所允许的CAN帧的接收周期的范围，所述CAN-ID是表示CAN帧的数据的种类的标识符。另外，第2规则也可以还表示在与多个CAN-ID的每一个对应的CAN帧中所允许的变化量，所述变化量是从该CAN帧的前一个CAN帧的数据值起的变化量。该CAN帧的前一个CAN帧指的是，在同一CAN-ID中，比该CAN帧早一定时(timing)接收到的CAN帧。

[0144] 具体而言，第2规则是表示如下情况的规则：在CAN-ID为“0xA1”的CAN帧中，如果参照在图12中说明的对E帧所附加的CAN帧的接收时刻算出的周期在基本周期10ms±3ms的范围内、也即是说与前一个接收到的CAN帧的接收时刻的差量在基本周期10ms±3ms的范围内，则为正确的周期。另外，第2规则也可以是表示在CAN-ID为“0xA1”的CAN帧中如果与前一个接收到的CAN帧的数据的变化量为±50则为正确的变化量这一情况的规则。对于其他ID也同样地定义了所允许的周期的范围以及数据的变化量。

[0145] 此外，在第2规则中定义的数据值的变化量是与车辆1的状态信息对应的数值，例如是车速的变化量、转向器的角度的变化量等。

[0146] 在使用第2规则的情况下，自动驾驶DCU100的异常检测处理部104使用分别与从由第2通信部101b接收到的E帧中获得的多个CAN帧对应的多个接收时刻，检测该E帧所包含的多个CAN帧是否异常。具体而言，异常检测处理部104通过对彼此具有相同的标识符的多个CAN帧中的、第1CAN帧的第1接收时刻和第2CAN帧的第2接收时刻进行比较来检测第1CAN帧是否有异常。异常检测处理部104在第1接收时刻和第2接收时刻的差量处于在第2规则中与上述相同的标识符相关联的接收周期的范围外的情况下，检测为第1CAN帧异常。

[0147] 另外，异常检测处理部104也可以在第1CAN帧的第1数据值和第2CAN帧的第2数据值的差量超过在第2规则中与上述相同的标识符相关联的变化量的情况下，检测为第1CAN帧异常。

[0148] 而且，异常检测处理部104在检测到CAN帧异常的情况下，禁止控制指令的转发。也即是说，异常检测处理部104在该情况下既可以禁止对在该时间点从自动驾驶ECU110接收到的控制指令的转发，也可以禁止对在该时间点以后从自动驾驶ECU110接收到的控制指令的转发。

[0149] 接下来，对实施方式2涉及的车辆1所搭载的网络系统3的工作进行说明。

[0150] 图14以及图15是表示实施方式2涉及的网络系统3中的异常检测方法的一例的时序图。在实施方式2涉及的异常检测方法中，关于步骤S200～S208，仅于在步骤S201中如图12所示的使E帧包含CAN帧的接收时刻之处与实施方式1涉及的异常检测方法的步骤S101不同，而其他的步骤S200、S202～S208与实施方式1涉及的异常检测方法中的S100、S102～S108是同样的，因此省略说明。

[0151] 在自动驾驶DCU100中，异常检测处理部104参照异常检测规则保持部105所保持的异常检测规则。在此参照的规则是图13所示的第2规则。

[0152] 在自动驾驶DCU100中，异常检测处理部104判定CAN帧是否异常(S210)。异常检测处理部104在判定为CAN帧异常的情况下(步骤S210：异常)，将处理移至步骤S213。异常检测处理部104在判定为CAN帧正常的情况下(步骤S210：正常)，将处理移至步骤S211。

[0153] 在自动驾驶DCU100中，异常检测处理部104由于检测到CAN帧的异常，因而判断为要继续进行自动控制则有高风险，并使用第2通信部101b向服务器2或者IVI310通知包含存在异常这一情况的信息(S213)。此外，在该情况下，异常检测处理部104不将控制指令发送给中央网关400。也即是说，异常检测处理部104在该情况下禁止将判定为异常的控制指令经由中央网关400以及CAN网关200向第2网络20转发。

[0154] 步骤S211、S212、S214以及S215分别与实施方式1涉及的异常检测方法中的步骤S109、S110、S112以及S113是同样的，因此省略说明。另外，步骤S221～S224与实施方式1涉及的异常检测方法中的S120～S123是同样的，因此省略说明。

[0155] 此外，虽然设成了在步骤S210之后进行步骤S212的流程，但也可以是在步骤S212之后进行步骤S210。

[0156] 在本实施方式涉及的异常检测装置中，异常检测规则还包含用于检测CAN帧是否异常的第2规则。异常检测处理部104进而在检测到CAN帧异常的情况下禁止控制指令的转发。由此，异常检测装置能够在检测了CAN帧的异常之后进行控制指令的执行。也即是说，能够在作为第1网络10侧的设备的异常检测装置中也确认了第2网络20侧是正常的之后对自动驾驶控制指令的发送进行判断。因此，即使在攻击了第2网络20的脆弱性的攻击期间，异常检测装置也能够防止不正常的自动驾驶控制。

[0157] 另外，在本实施方式涉及的异常检测装置中，第2规则表示在与多个标识符的每一个对应的CAN帧中所允许的CAN帧的接收周期的范围。第2通信部101b接收保存了多个CAN帧和接收时刻作为数据的E帧，所述接收时刻是多个CAN帧的每一个由第1网络10上的设备接收到的时刻。异常检测处理部104使用分别与多个CAN帧对应的多个接收时刻，在彼此具有相同的标识符的多个CAN帧之中，在第1CAN帧的第1接收时刻与比第1CAN帧早一帧接收到的第2CAN帧的第2接收时刻的差量位于在第2规则中与上述相同的标识符相关联的接收周期的范围外的情况下，检测为第1CAN帧异常。由此，利用异常检测装置，即使是在第2网络20上发生了异常的情况下，也能够在第1网络10中的设备中检测具有周期性的CAN帧的异常，因此能够停止自动驾驶。

[0158] 另外，在本实施方式涉及的异常检测装置中，第2规则还表示在与多个所述标识符的每一个对应的CAN帧中所允许的从前一个CAN帧的数据值起的变化量。异常检测处理部104进而在第1CAN帧的第1数据值与第2CAN帧的第2数据的差量超过在第2规则中与上述相同的标识符相关联的变化量的情况下，检测为第1CAN帧异常。由此，利用异常检测装置，即使是在第2网络20上发生了异常的情况下，也能够在第1网络10中的设备中检测CAN帧的数据值的异常，因此能够停止自动驾驶。

[0159] (实施方式3)

[0160] 接着对实施方式3进行说明。实施方式3涉及的作为异常检测装置的自动驾驶DCU100与实施方式2涉及的自动驾驶DCU在进行CAN帧的异常检测之处大致相同，而不同之处在于，前者使得能够在E帧内指定异常检测的规则。

[0161] 图16是表示实施方式3涉及的CAN网关200基于接收到的多个CAN帧来发送E帧的样

子的图。

[0162] 图17是表示定义了在实施方式3涉及的自动驾驶DCU100中进行CAN的异常检测时的异常检测规则的表的图。

[0163] 在图16的E帧中，如果是定义了规则1作为异常检测规则的CAN帧，则自动驾驶DCU100的异常检测处理部104检查(check)与该CAN帧具有相同的CAN-ID的CAN帧的周期来进行异常检测。异常检测处理部104在使用规则1的情况下，使用在实施方式2中说明的参照CAN帧的接收时刻算出的周期和第2规则来进行异常检测。

[0164] 另外，如果是定义了规则2作为检测规则的CAN帧，则自动驾驶DCU100的异常检测处理部104检查该CAN帧的数据值的变化量来进行异常检测。异常检测处理部104在使用规则2的情况下，使用在实施方式2中说明的CAN帧的数据值和第2规则来进行异常检测。

[0165] 另外，如果是定义了规则3作为检测规则的CAN帧，则自动驾驶DCU100的异常检测处理部104检查该CAN帧的消息认证码(Message Authentication Code)来进行异常检测。在规则3的情况下，以自动驾驶DCU100事先共享有用于进行认证的MAC密钥为前提。也即是说，在该情况下，异常检测处理部104在消息认证码与MAC密钥一致时判断为正常，否则判断为异常。

[0166] 如此，异常检测处理部104取得与多个标识符的每一个相关联的规则作为异常检测规则。而且，异常检测处理部104参照异常检测规则来检测CAN帧异常。

[0167] 由此，异常检测装置能够按每个CAN帧设定检测规则。例如在第2网络20侧的负荷高、难以在第2网络20侧进行检测处理的情况下，能够通过第1网络10上的设备检测第2网络20中的异常。

[0168] 此外，CAN网关200也可以接收多个CAN帧，并对接收到的多个CAN帧的每一个附加与该CAN帧的CAN-ID相关联的异常检测的规则。在此，CAN网关200附加的异常检测的规则例如也可以是实施方式2的图13中说明的第2规则。CAN网关200既可以附加第2规则中的对应于CAN-ID的规则，也可以附加第2规则的全部。

[0169] 另外，图17中说明的异常检测规则也可以由自动驾驶DCU100的异常检测规则保持部105保持，在该情况下，按每个CAN-ID关联有该异常检测规则。

[0170] (其他实施方式)

[0171] 如上所述，作为本公开涉及的技术的例示，说明了实施方式1～3。然而，本公开涉及的技术不限定于此，也能够适用于适当进行了变更、替换、附加、省略等的实施方式。例如，如下的变形例也包含在本公开的一个实施方式中。

[0172] (1)在上述实施方式中，在车载网络中遵循CAN协议进行数据帧的传输，但CAN协议可以作为包含在自动化系统等中使用的CANOpen、或TTCAN(Time-Triggered CAN:时间触发CAN)、CANFD(CAN with Flexible Data Rate:灵活的数据速率)等派生的协议在内的广义的含义来对待。另外，车载网络也可以使用CAN协议以外的协议。作为进行用于车辆的控制的帧等的传输的车载网络的协议，例如也可以使用LIN(Local Interconnect Network:局域互联网)、MOST(注册商标)(Media Oriented Systems Transport)、FlexRay(注册商标)、Ethernet(注册商标)等。另外，也可以将使用这些协议的网络作为子网络，组合多种协议涉及的子网络来构成车载网络。另外，Ethernet(注册商标)协议可以作为包含IEEE802.1涉及的Ethernet(注册商标)AVB(Audio Video Bridging:音视频桥接)或

IEEE802.1涉及的Ethernet(注册商标)TSN(Time Sensitive Networking:时间敏感网络)、Ethernet(注册商标)/IP(Industrial Protocol:工业协议)、EtherCAT(注册商标)(Ethernet(注册商标)for Control Automation Technology)等派生协议在内的广义的含义来对待。此外,车载网络的网络总线例如可以是由电线、光纤等构成的有线通信线路。例如也可以为,帧传输阻止装置2400在ECU使用上述的某个协议进行通信的网络系统中连接于网络总线,接收帧,并基于表示是否容许阻止帧的传输的管理信息,切换是否执行在接收到的帧满足预定条件的情况下阻止该帧的传输的预定处理。

[0173] (2)在上述实施方式中,以标准ID格式记述了CAN协议中的数据帧,但也可以是扩展ID格式,数据帧的ID也可以是扩展ID格式下的扩展ID等。另外,上述的数据帧也可以是使用除CAN以外的协议的网络中的一种帧,在该情况下,识别该帧的种类等的ID相当于数据帧的ID。

[0174] (3)在上述实施方式中,防止了自动驾驶控制指令的不正(不正常),但也可以使得检测停车辅助系统、车道保持功能、防撞功能等先进驾驶辅助系统的控制的异常。

[0175] (4)在上述实施方式中,异常检测时向服务器2和/或IVI(In-Vehicle Infotainment)310进行了异常通知,而如果能够进行V2X(车联网)和/或V2I(车路通信)的通信,如果对应于车车间通信和/或车路间通信,也可以向其他车辆进行异常通知、向基础设施装置进行异常通知。由此能够向本车周边的车辆和/或行人所保有的设备通知异常,能够至使防止事故发生。

[0176] (5)在上述实施方式中,异常检测时向服务器2和/或IVI(In-Vehicle Infotainment)310进行了异常通知,但也可以使得作为日志留在车载网络上的设备中。在留在了日志中的情况下,通过从诊断端口读取日志,经销商能够掌握异常内容。另外,也可以将日志定期发送到服务器2。由此,能够远程进行车辆的异常检测。

[0177] (6)在上述实施方式中,CAN网关将车辆的状态信息的CAN帧保存于E帧的数据,而如果车辆的状态信息是能够识别的形式,则也可以不是CAN帧的格式。

[0178] (7)在上述实施方式中,自动驾驶DCU100没有与第2传输线路21连接,但自动驾驶DCU也可以与第2传输线路连接。在该情况下,也可以读入在第2传输线路上流通的CAN帧,接收车辆的状态信息。再者,在该情况下,也可以使得自动驾驶控制指令也直接向第2传输线路发送。

[0179] (8)在上述实施方式中,图9的自动驾驶的控制指令的异常检测规则或者图13的异常检测规则作为白名单而定义了正常的条件,但也可以是作为黑名单而被定义的第3规则。

[0180] 例如,在实施方式2中,也可以取代定义了白名单的第2规则而使用定义了黑名单的第3规则作为异常检测规则。

[0181] 第3规则表示在与CAN-ID对应的CAN帧中所允许的CAN帧的接收周期的范围,所述CAN-ID是表示CAN帧的数据的种类的标识符。另外,第3规则还表示在与多个所述标识符的每一个对应的CAN帧中所允许的变化量,所述变化量是从该CAN帧的前一个CAN帧的数据值的变化量。

[0182] 在使用第3规则的情况下,自动驾驶DCU100的异常检测处理部104使用分别与从由第2通信部101b接收到的E帧中获得的多个CAN帧对应的多个接收时刻,检测该E帧所包含的多个CAN帧是否异常。具体而言,异常检测处理部104通过对彼此具有相同的标识符的多个

CAN帧中的、第1CAN帧的第1接收时刻和第2CAN帧的第2接收时刻进行比较来检测第1CAN帧是否有异常。异常检测处理部104在第1接收时刻和第2接收时刻的差量处于在第2规则中与上述相同的标识符相关联的接收周期的范围内的情况下，检测为第1CAN帧异常。

[0183] 由此，利用异常检测装置，即使是在第2网络20上发生了异常的情况下，也能够在第1网络10中的设备中检测具有周期性的CAN帧的异常，因此能够停止自动驾驶。

[0184] 另外，异常检测处理部104也可以在所述第1CAN帧的第1数据值和第2CAN帧的第2数据值的差量处于在第3规则中与所述相同的标识符相关联的变化量的范围内的情况下，检测为第1CAN帧异常。

[0185] 由此，利用异常检测装置，即使是在第2网络20上发生了异常的情况下，也能够在第1网络10中的设备中检测CAN帧的数据值的异常，因此能够停止自动驾驶。

[0186] 另外，异常检测规则也可以为，将白名单和黑名单合起来进行异常检测。

[0187] (9)在上述实施方式中，图8的交换规则以白名单形式定义了正常的发送源、发送目的地的IP和MAC地址以及端口号，但也可以定义为黑名单。另外，作为交换规则所定义的规则，也可以定义流量、通信频度、有效载荷的值的条件。

[0188] (10)在上述实施方式中，表示了帧异常检测装置搭载于车辆且包含于进行用于车辆控制的通信的车载网络系统的例子，但也可以包含于用于车辆以外的移动体控制对象的控制的网络系统。也即是说，移动体例如是机器人、航空器、船舶、机器、建筑设备、农业设备、无人机等。

[0189] (11)上述实施方式中示出的ECU等各装置也可以除了存储器、处理器等之外还具备硬盘单元、显示器单元、键盘、鼠标等。另外，上述实施方式中示出的ECU等各装置既可以由处理器执行存储于存储器的程序以软件方式来实现其各装置的功能，也可以不使用程序而通过专用的硬件(数字电路等)来实现其功能。另外，该各装置内的各构成要素的功能分担可以变更。

[0190] (12)构成上述实施方式中的各装置的构成要素的一部分或者全部也可以由1个系统LSI(Large Scale Integration:大规模集成电路)构成。系统LSI是将多个结构部分集成在1个芯片上而制造出的超多功能LSI，具体而言，是构成为包括微处理器、ROM、RAM等的计算机系统。RAM中记录有计算机程序。微处理器按照计算机程序进行工作，由此系统LSI实现其功能。另外，构成上述各装置的构成要素的各部既可以单独地单芯片化，也可以以包含一部分或全部的方式单芯片化。另外，虽然此处设为系统LSI，但根据集成度不同，也可以称为IC、LSI、超大LSI(super LSI)、特大LSI(ultra LSI)。另外，集成电路化的方法不限于LSI，也可以通过专用电路或者通用处理器实现。也可以在LSI制造后利用可编程的FPGA(Field Programmable Gate Array:现场可编程门阵列)、可以对LSI内部的电路单元的连接和/或设定进行重构的可重构处理器(reconfigurable processor)。进而，随着半导体技术的进步或者派生的其他技术的出现，如果出现能够替代LSI的集成电路化的技术，当然也可以利用该技术进行功能块的集成化。也可能会存在适用生物技术等的可能性。

[0191] (13)构成上述各装置的构成要素的一部分或全部也可以由能够装卸于各装置的IC卡或单体模块构成。IC卡或所述模块是由微处理器、ROM、RAM等构成的计算机系统。IC卡或所述模块也可以包括上述的超多功能LSI。微处理器按照计算机程序进行工作，由此IC卡或模块实现其功能。该IC卡或该模块可以具有防篡改性能。

[0192] (14)作为本公开的一个技术方案，也可以是通过计算机实现异常检测方法的程序(计算机程序)，还可以是由所述计算机程序形成的数字信号。另外，作为本公开的一个技术方案，也可以将所述计算机程序或者所述数字信号记录于计算机可读取的记录介质例如软盘、硬盘、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、BD(Blu-ray(注册商标)Disc)、半导体存储器等。另外，也可以是记录在这些记录介质中的数字信号。另外，作为本公开的一个技术方案，也可以将计算机程序或数字信号经由电通信线路、无线或有线通信线路、以互联网为代表的网络、数据广播等进行传输。另外，作为本公开的一个技术方案，也可以是具备微处理器和存储器的计算机系统，存储器记录有上述计算机程序，微处理器按照计算机程序进行工作。另外，也可以通过将程序或数字信号记录在记录介质中转移、或经由网络等将程序或数字信号进行转移，由此通过独立的其他的计算机系统来实施。

[0193] (15)通过将上述实施方式及上述变形例中示出的各构成以及功能任意地进行组合而实现的方式也包含在本公开的范围内。

[0194] 产业上的可利用性

[0195] 本公开涉及的异常检测装置作为能够有效地检测异常的异常检测装置以及异常检测方法等是有用的。

[0196] 标号说明

[0197] 1车辆;2服务器;3网络系统;10第1网络;11第1传输线路;20第2网络;21第2传输线路;21a、21b CAN总线;30外部网络;100自动驾驶DCU;101a第1通信部;101b第2通信部;102交换处理部;103交换规则保持部;104异常检测处理部;105异常检测规则保持部;110自动驾驶ECU;120摄像头;130LIDAR;140动态地图ECU;200CAN网关;201E收发部;202a、202b CAN收发部;203转发控制部;204转发规则保持部;210发动机ECU;220转向器ECU;230制动器ECU;240车窗ECU;300信息娱乐DCU;310IVI;400中央网关;410远程信息控制单元;420诊断端口;P1～P5端口。

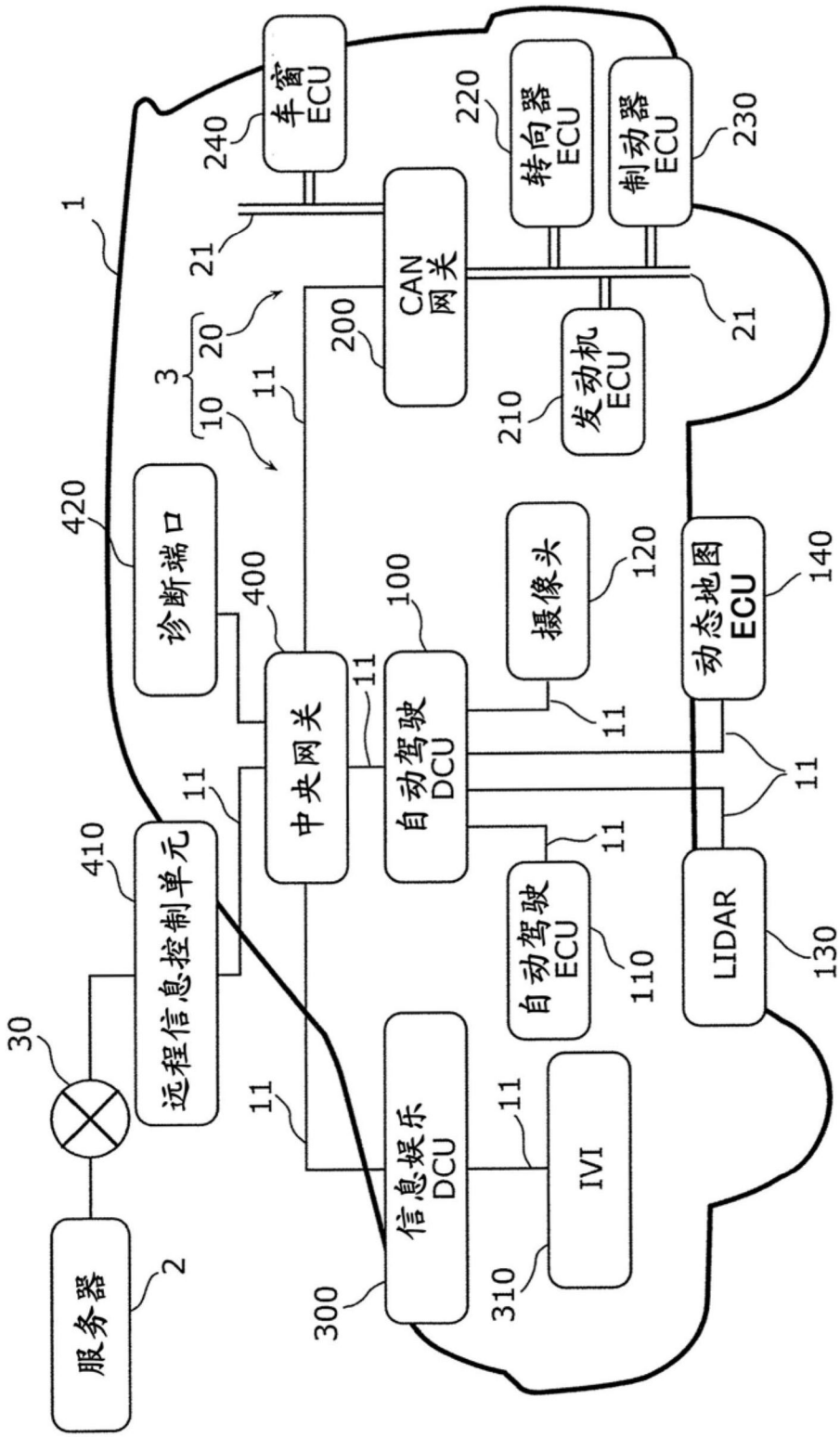

服务器
2
30
远程信息控制单元
410
420
诊断端口
中央网关
400
11
自动驾驶DCU
100
信息娱乐DCU
300
IVI
310
自动驾驶ECU
110
摄像头
120
LIDAR
130
动态地图ECU
140
CAN网关
200
车窗ECU
240
转向器ECU
220
制动器ECU
230
发动机ECU
210
1
3
10
20
21

图1

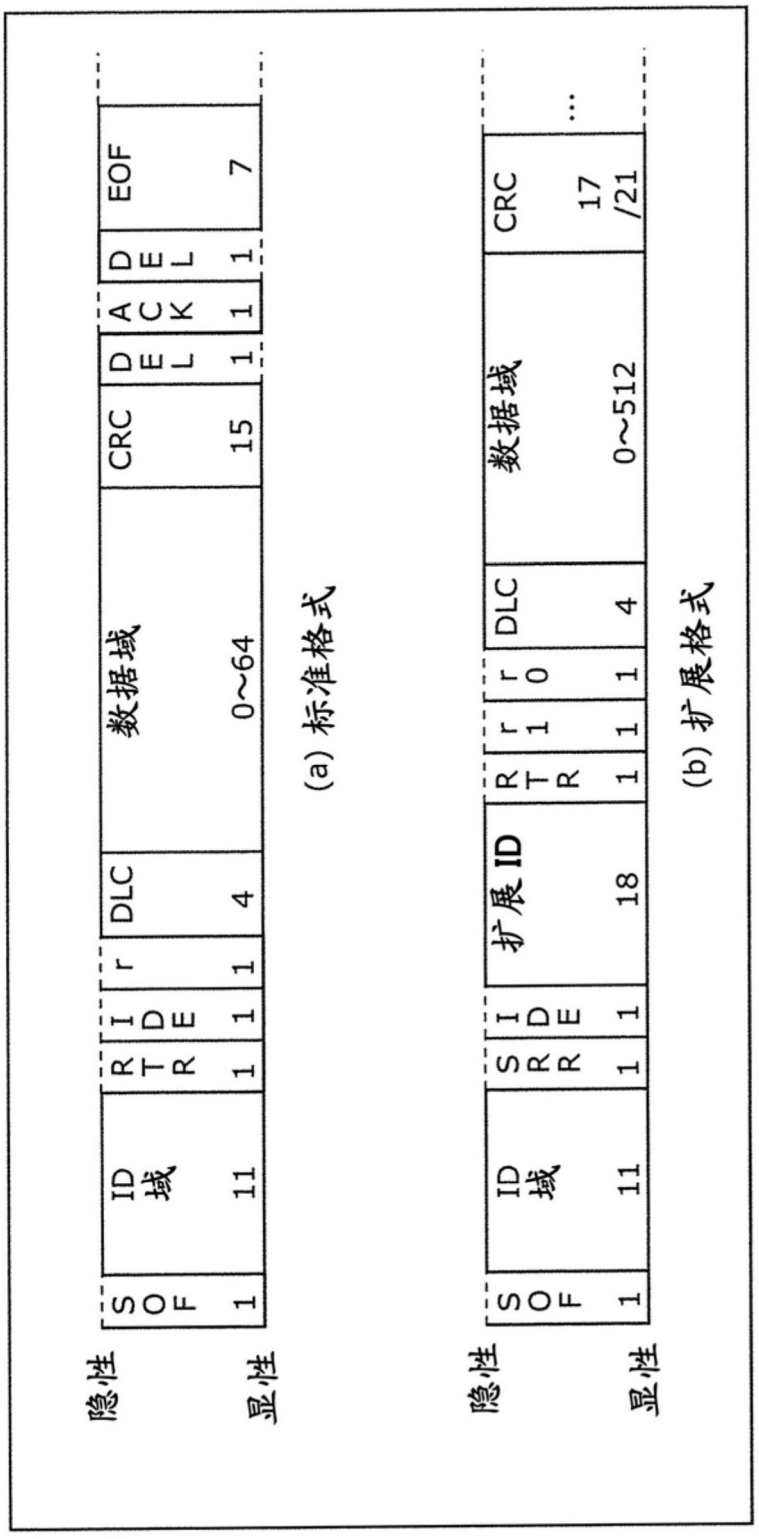

隐性
显性
SOF
1
ID域
11
RTR
1
IDE
1
r
1
DLC
4
数据域
0~64
CRC
15
DEL
1
ACK
1
DEL
1
EOF
7
(a) 标准格式
隐性
显性
SOF
1
ID域
11
SRR
1
IDE
1
扩展ID
18
RTR
1
r1
1
r0
1
DLC
4
数据域
0~512
CRC
17
/21
...
(b) 扩展格式

图2

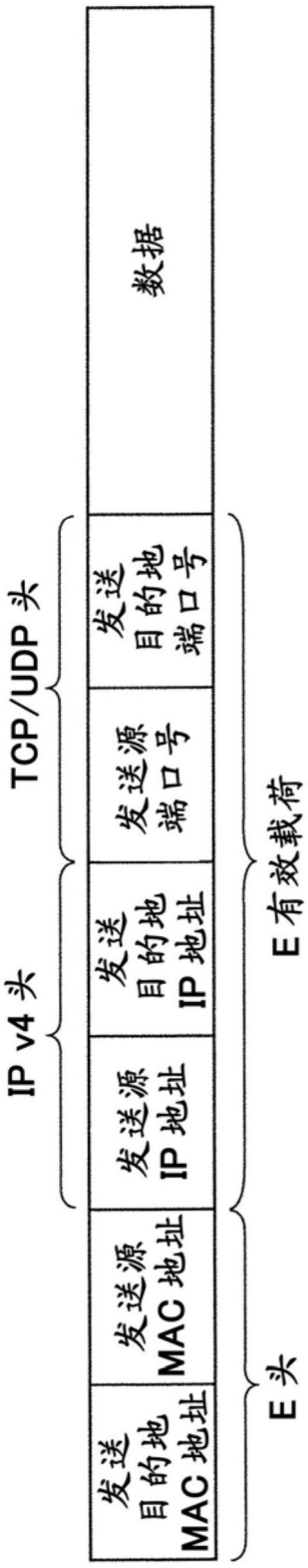

发送目的地MAC地址
发送源MAC地址
发送源IP地址
发送目的地IP地址
发送源端口号
发送目的地端口号
数据
E 头
IP v4 头
TCP/UDP 头
E 有效载荷

图3

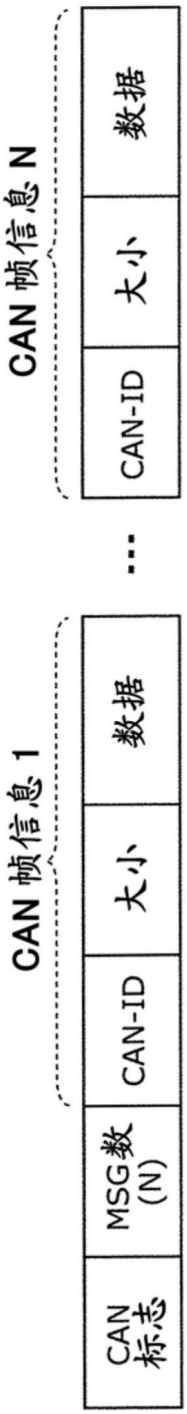


图4

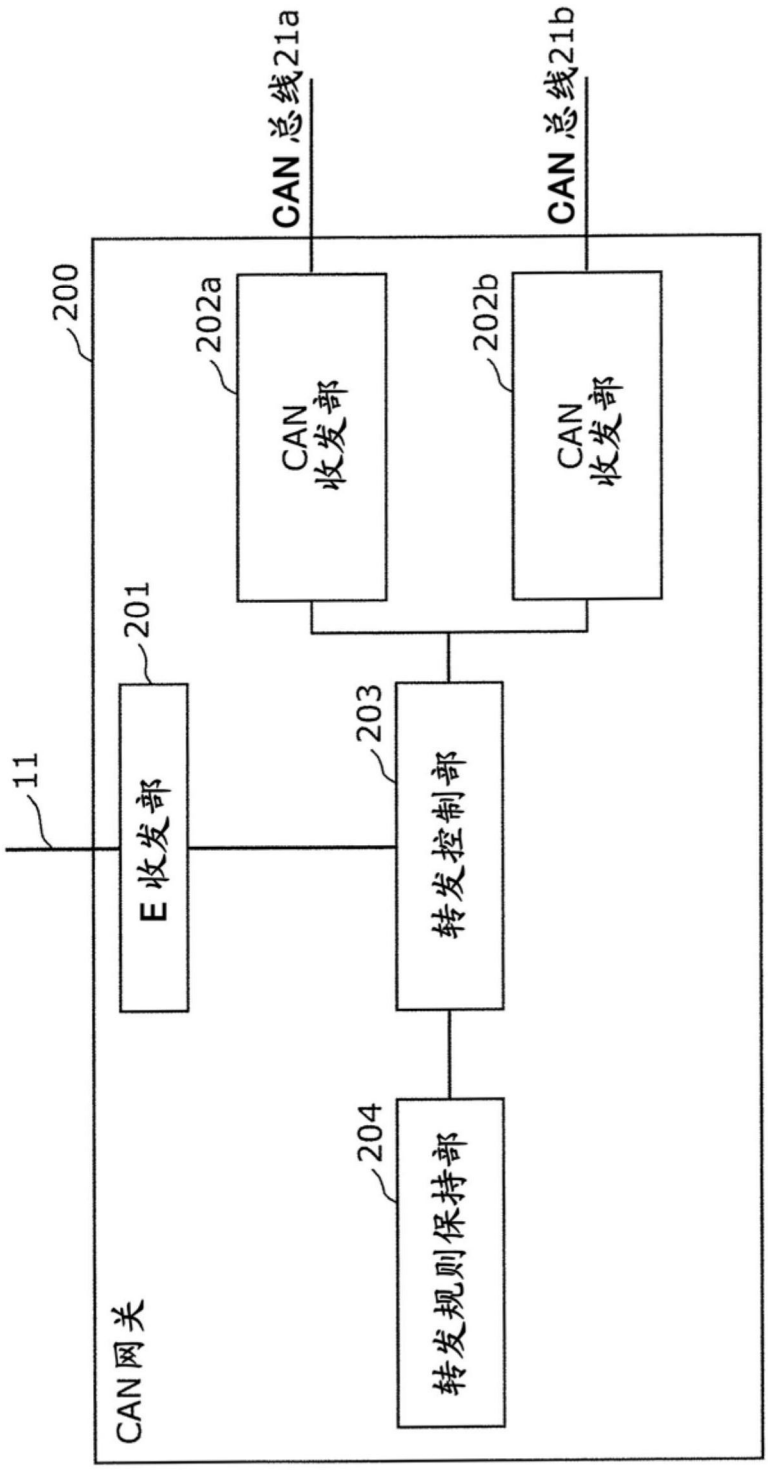

CAN 总线21a
CAN 总线21b
200
202a
CAN
收发部
202b
CAN
收发部
201
E 收发部
11
203
转发控制部
204
转发规则保持部
CAN 网关

图5

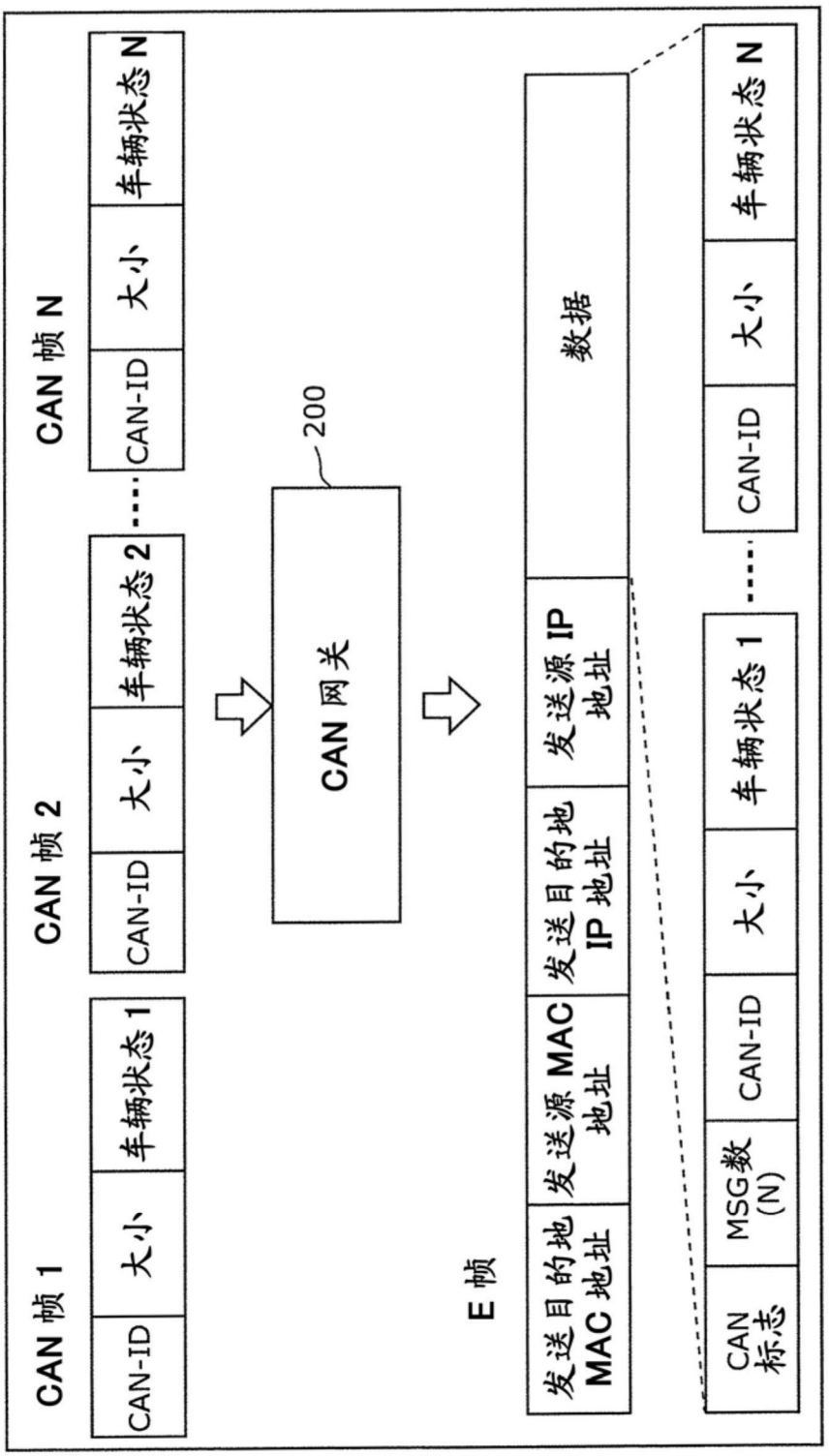

CAN 帧 1
CAN-ID
大小
车辆状态 1
CAN 帧 2
CAN-ID
大小
车辆状态 2
CAN 帧 N
CAN-ID
大小
车辆状态 N
200
CAN 网关
E 帧
发送目的地 MAC 地址
发送源 MAC 地址
发送目的地 IP 地址
发送源 IP 地址
数据
CAN 标志
MSG数 (N)
CAN-ID
大小
车辆状态 1
CAN-ID
大小
车辆状态 N

图6

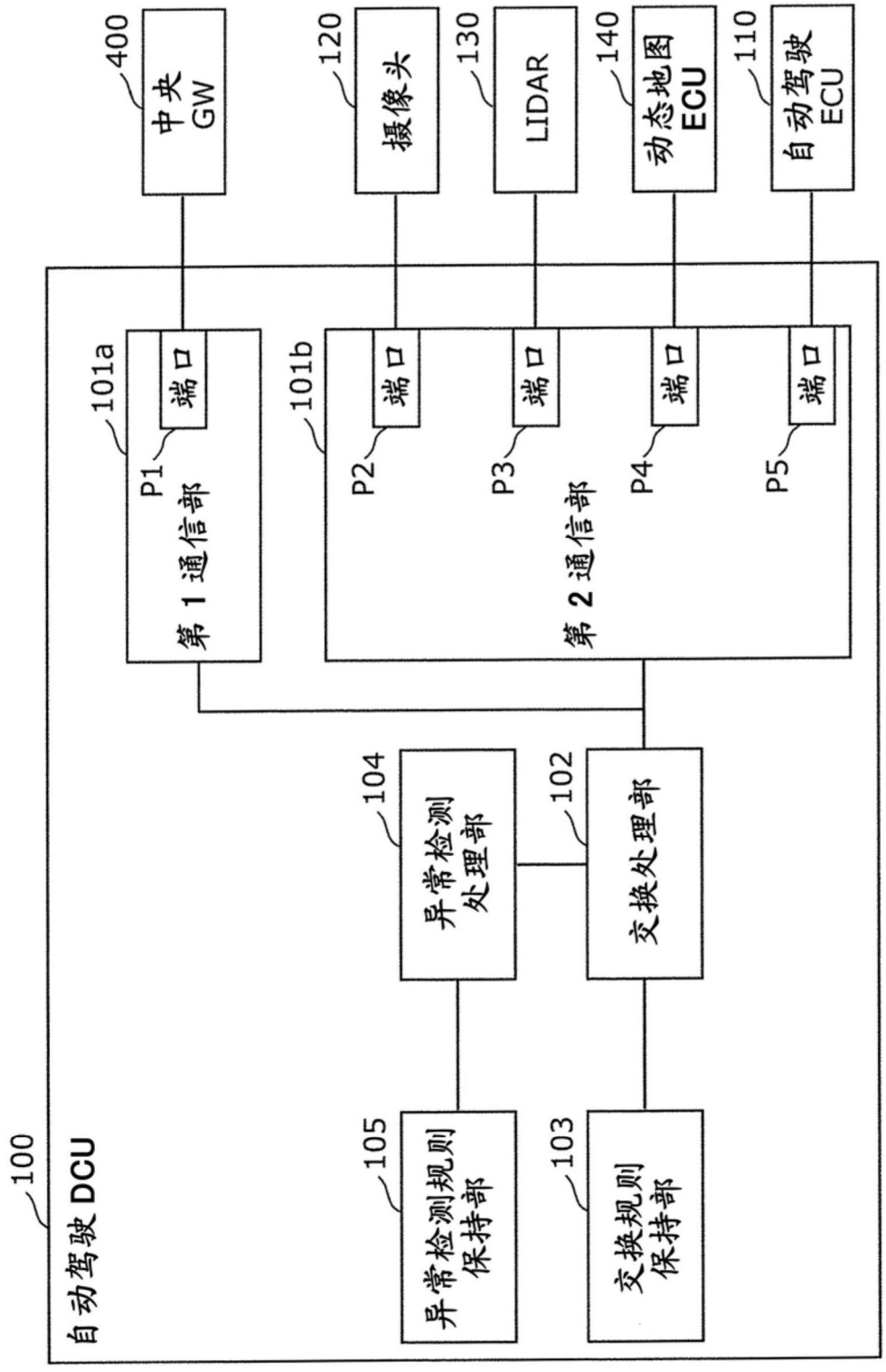

400
中央
GW
120
摄像头
130
LIDAR
140
动态地图
ECU
110
自动驾驶
ECU
100
自动驾驶 DCU
101a
端口
P1
第 1 通信部
101b
端口
P2
端口
P3
端口
P4
端口
P5
第 2 通信部
104
异常检测
处理部
102
交换处理部
105
异常检测规则
保持部
103
交换规则
保持部

图7

输入端口	发送源 IP 地址	发送源 MAC 地址	输出端口	发送目的地 IP 地址	发送目的地 MAC 地址
P1	CAN 网关	中央网关	P5	自动驾驶 ECU	自动驾驶 ECU
P2	摄像头	摄像头	P5	自动驾驶 ECU	自动驾驶 ECU
P3	LIDAR	LIDAR	P5	自动驾驶 ECU	自动驾驶 ECU
P4	动态地图 ECU	动态地图 ECU	P5	自动驾驶 ECU	自动驾驶 ECU
P5	自动驾驶 ECU	自动驾驶 ECU	P1	CAN 网关	中央网关
P2	摄像头	摄像头	P1	IVI	信息娱乐 DCU
P4	动态地图	动态地图	P1	地图服务器	中央网关
P3	摄像头	摄像头	P1	地图服务器	中央网关
-	自动驾驶 DCU	自动驾驶 DCU	P1	监视服务器	中央网关

图8

车速状态	换挡状态	车速指示	操舵指示
低速	D	⊿10km	⊿360度
中速	D	⊿20km	⊿180度
高速	D	⊿30km	⊿90度

图9

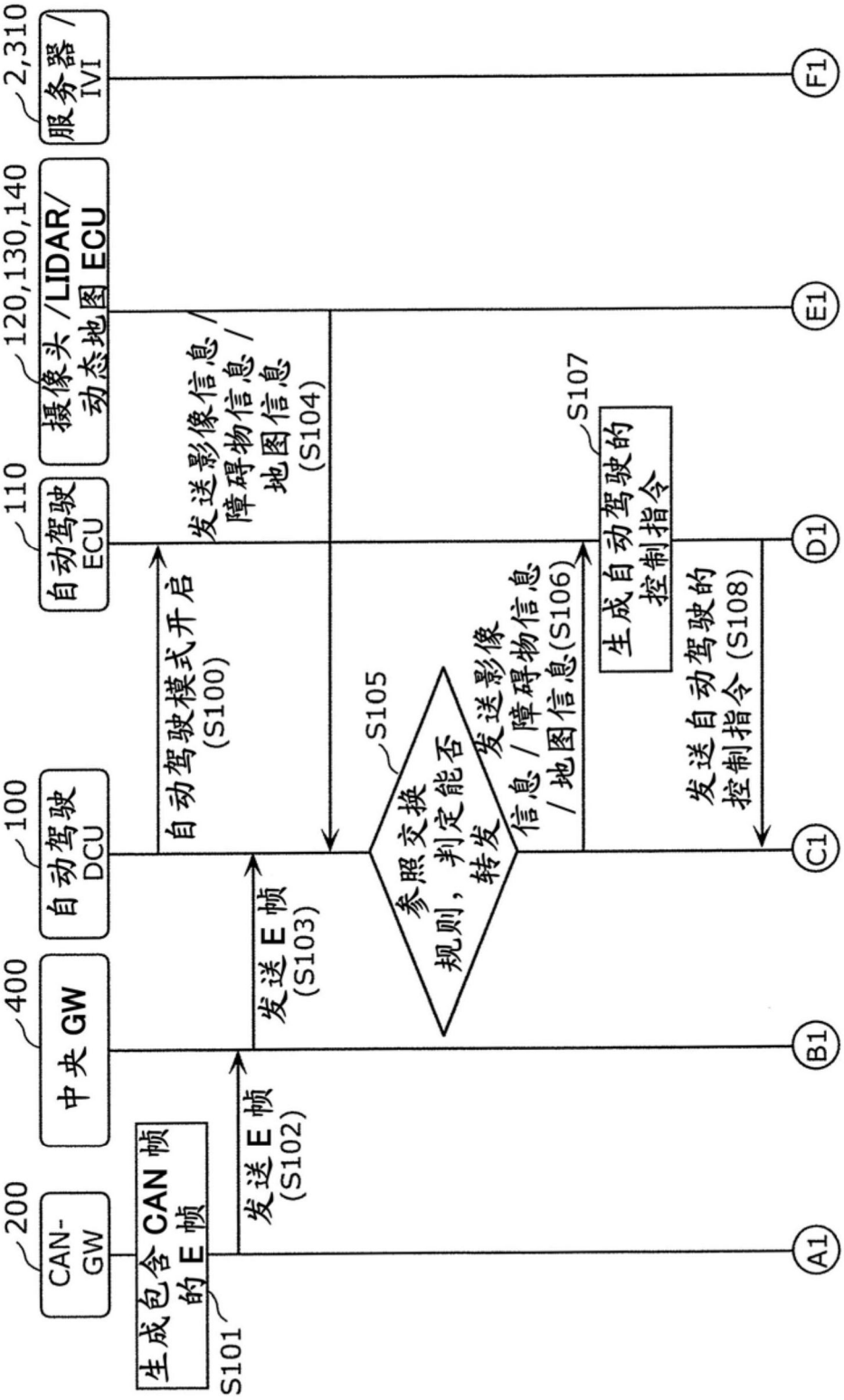

200
CAN-GW
400
中央 GW
100
自动驾驶 DCU
110
自动驾驶 ECU
120,130,140
摄像头 /LIDAR/ 动态地图 ECU
2,310
服务器 / IVI
生成包含 CAN 帧的 E 帧
S101
发送 E 帧 (S102)
发送 E 帧 (S103)
自动驾驶模式开启 (S100)
发送影像信息 / 障碍物信息 / 地图信息 (S104)
S105
参照交换规则，判定能否转发
发送影像信息 / 障碍物信息 / 地图信息(S106)
S107
生成自动驾驶的控制指令
发送自动驾驶的控制指令 (S108)
A1
B1
C1
D1
E1
F1

图10

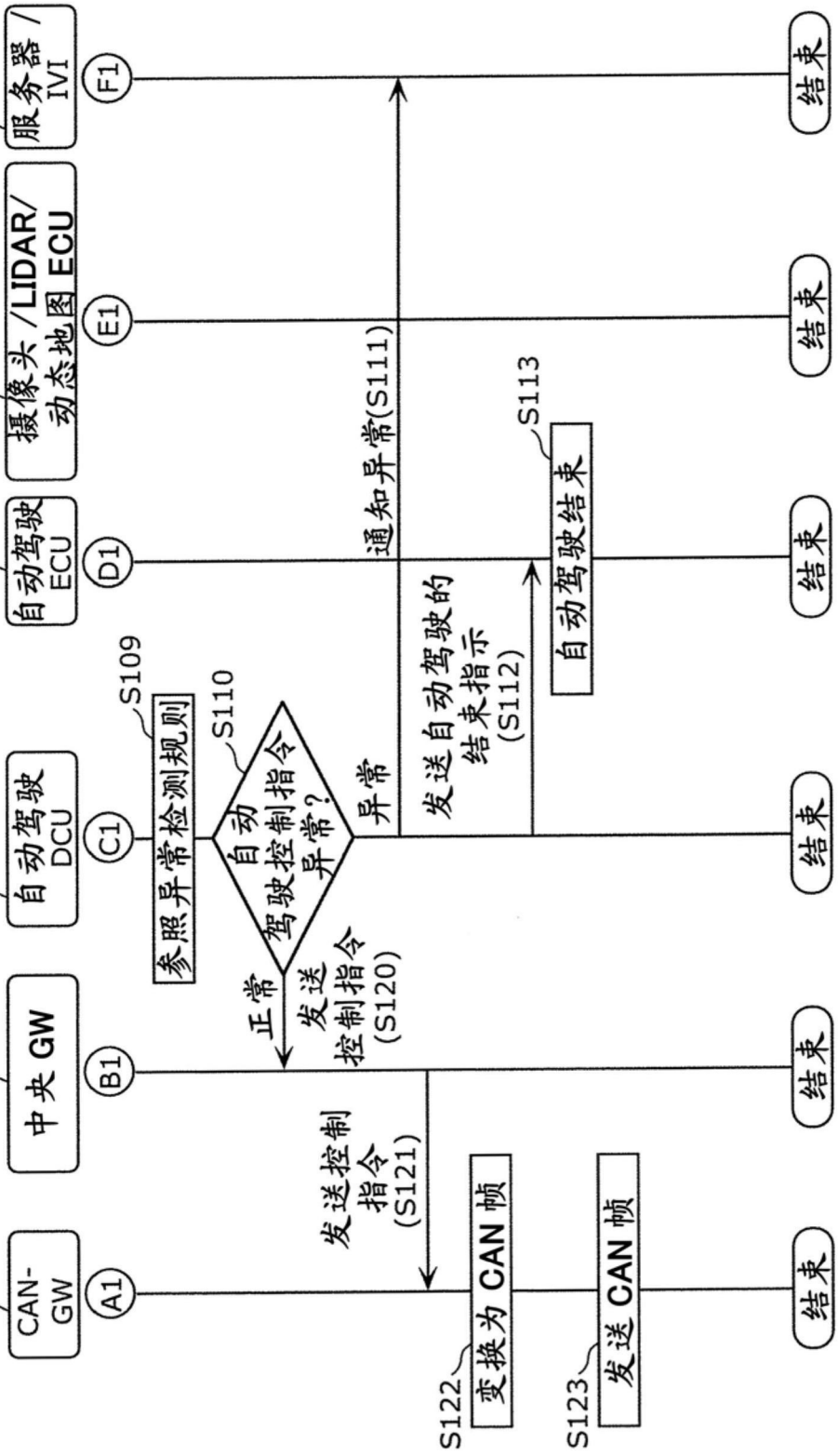

2,310
服务器 / IVI
F1
120,130,140
摄像头 /LIDAR/ 动态地图 ECU
E1
110
自动驾驶 ECU
D1
100
自动驾驶 DCU
C1
400
中央 GW
B1
200
CAN-GW
A1
S109
参照异常检测规则
S110
自动驾驶控制指令异常?
正常
异常
发送控制指令 (S120)
通知异常(S111)
发送自动驾驶的结束指示 (S112)
S113
自动驾驶结束
发送控制指令 (S121)
S122
变换为 CAN 帧
S123
发送 CAN 帧
结束
结束
结束
结束
结束
结束

图11

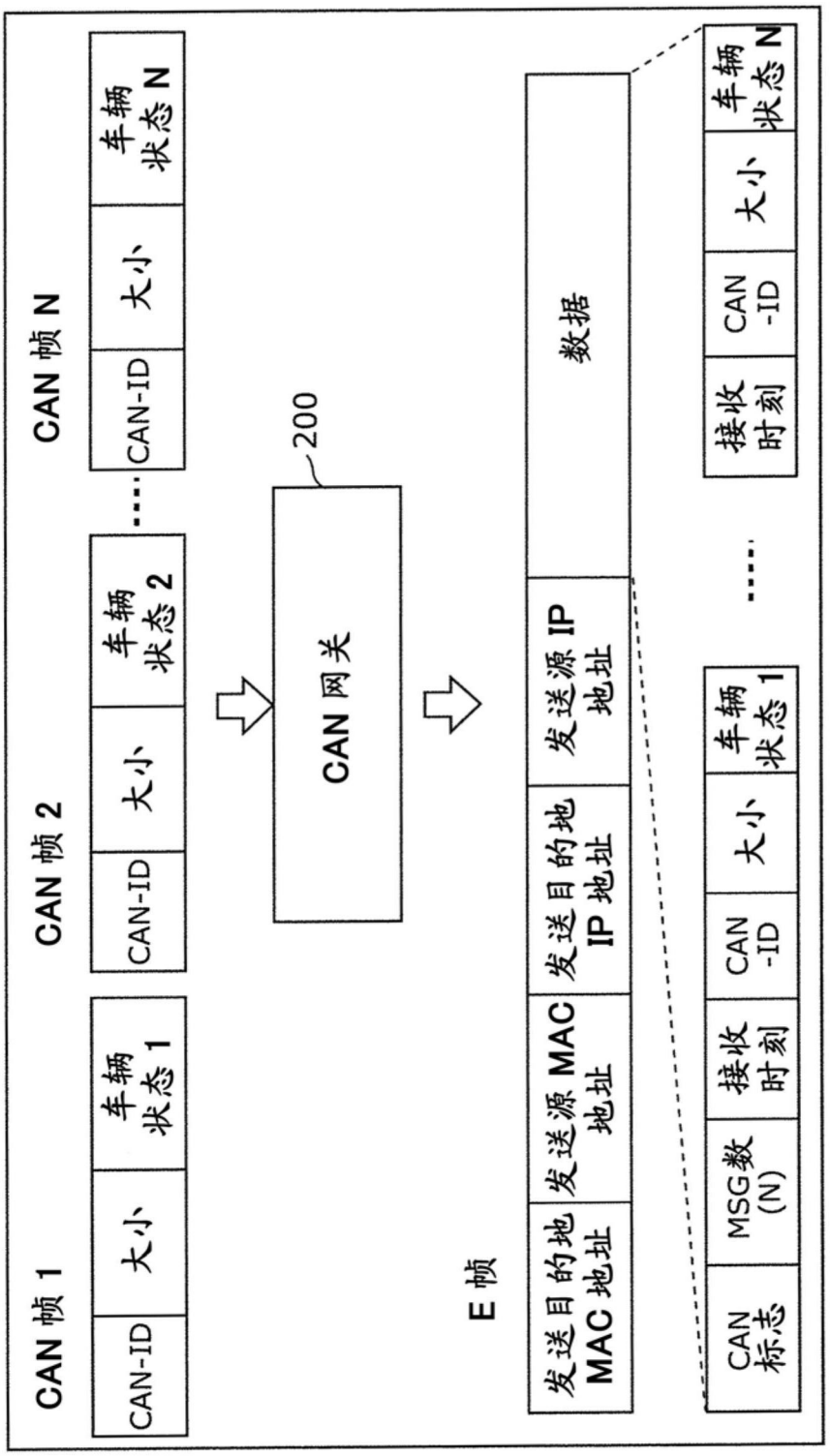

CAN 帧 1
CAN-ID
大小
车辆状态 1
CAN 帧 2
CAN-ID
大小
车辆状态 2
CAN 帧 N
CAN-ID
大小
车辆状态 N
200
CAN 网关
E 帧
发送目的地 MAC 地址
发送源 MAC 地址
发送目的地 IP 地址
发送源 IP 地址
数据
CAN 标志
MSG数 (N)
接收时刻
CAN -ID
大小
车辆状态 1
接收时刻
CAN -ID
大小
车辆状态 N

图12

CAN-ID	周期	周期余裕	数据值的变化量
0xA1	10ms	±3ms	±50
0xA2	20ms	±5ms	±100
0xA3	30ms	±10ms	±200

图13

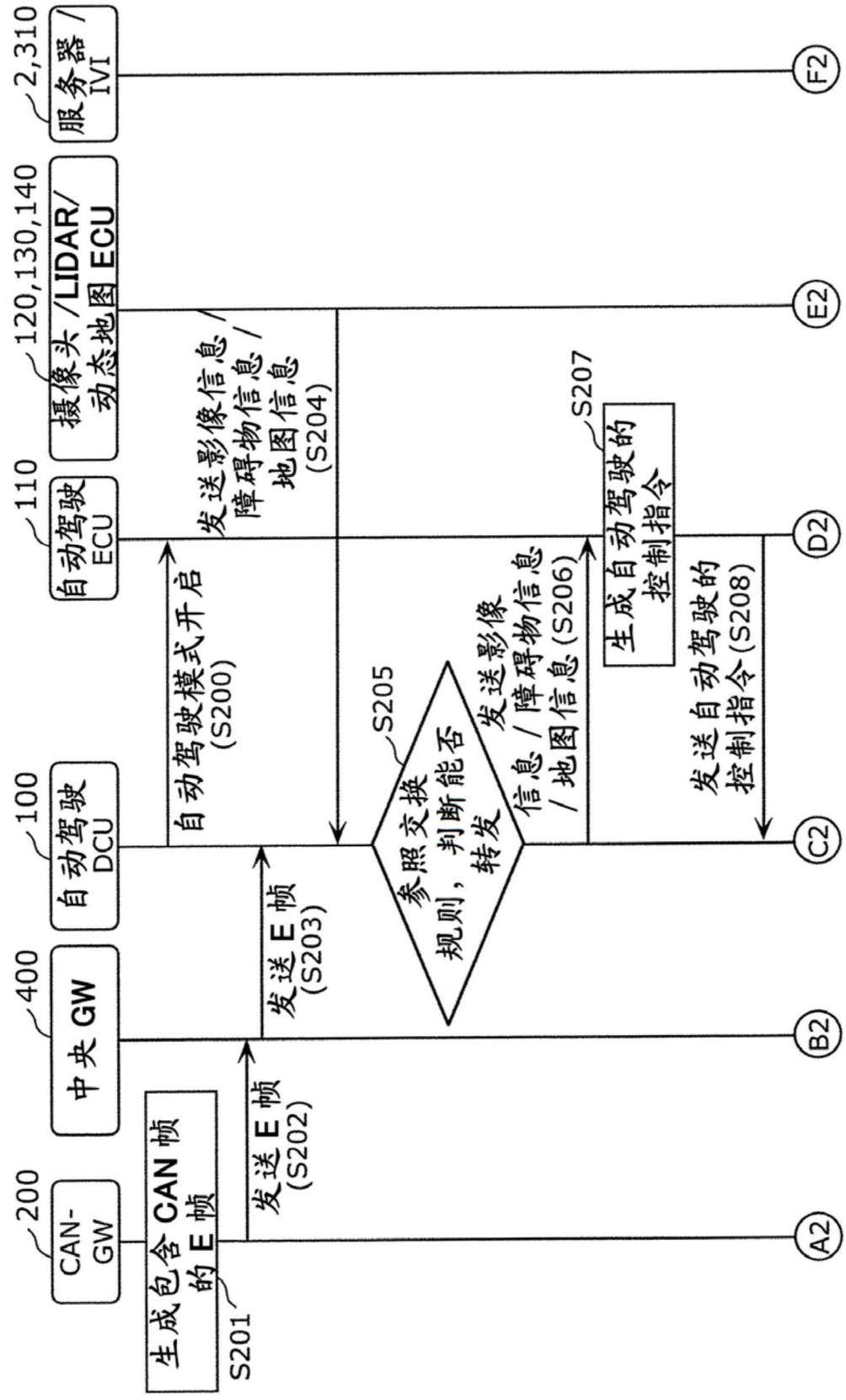

200
CAN-GW
400
中央 GW
100
自动驾驶 DCU
110
自动驾驶 ECU
120,130,140
摄像头 /LIDAR/ 动态地图 ECU
2,310
服务器 / IVI
生成包含 CAN 帧的 E 帧
S201
发送 E 帧 (S202)
发送 E 帧 (S203)
自动驾驶模式开启 (S200)
发送影像信息 / 障碍物信息 / 地图信息 (S204)
S205
参照交换规则，判断能否转发
发送影像信息 / 障碍物信息 / 地图信息 (S206)
S207
生成自动驾驶的控制指令
发送自动驾驶的控制指令 (S208)
A2
B2
C2
D2
E2
F2

图14

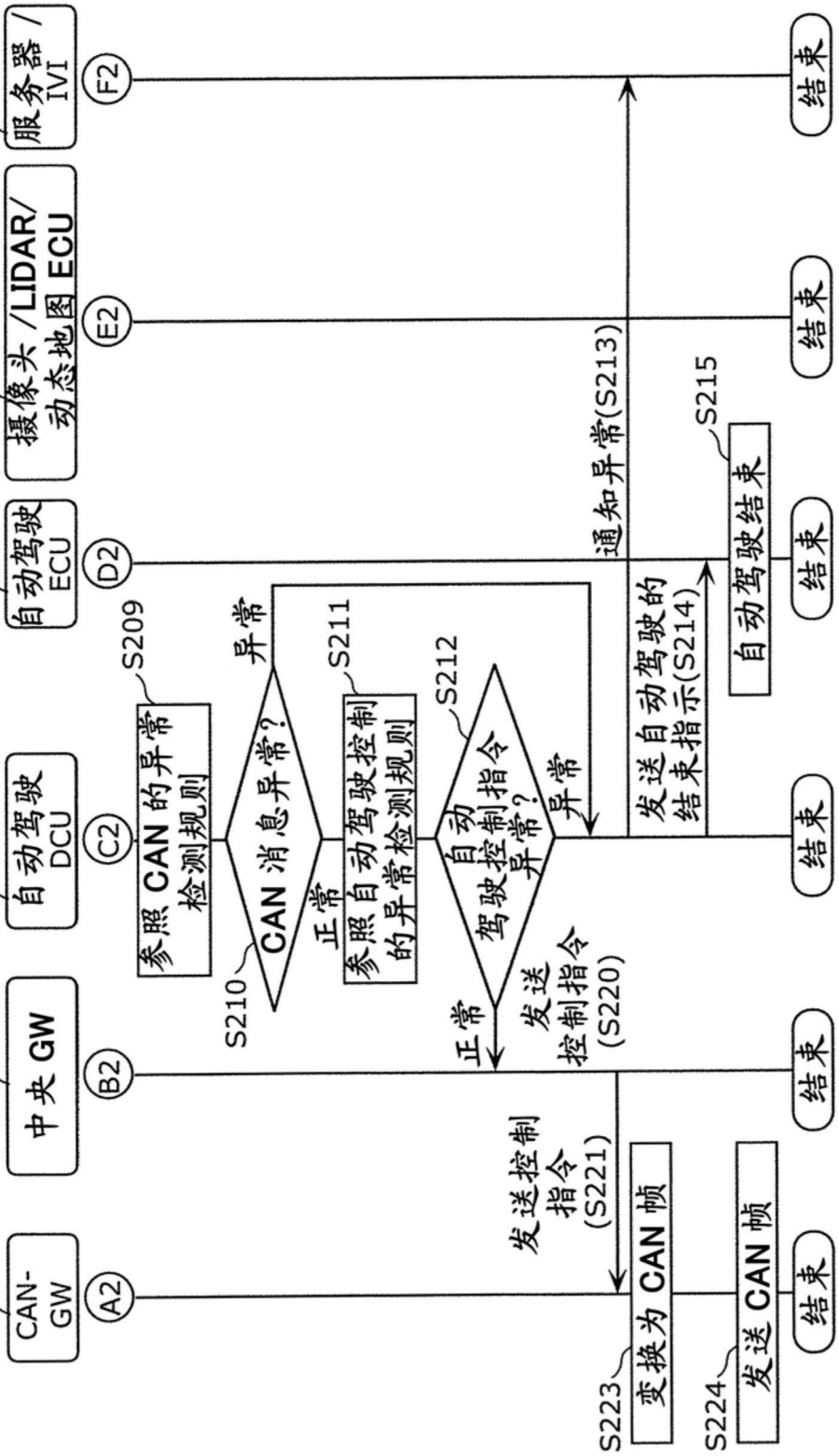

2,310
服务器 / IVI
F2
120,130,140
摄像头 /LIDAR/ 动态地图 ECU
E2
110
自动驾驶 ECU
D2
100
自动驾驶 DCU
C2
400
中央 GW
B2
200
CAN-GW
A2
S209
参照 CAN 的异常检测规则
S210
CAN 消息异常?
异常
正常
S211
参照自动驾驶控制的异常检测规则
S212
自动驾驶控制指令异常?
异常
正常
通知异常(S213)
发送自动驾驶的结束指示(S214)
S215
自动驾驶结束
发送控制指令(S220)
发送控制指令(S221)
S223
变换为 CAN 帧
S224
发送 CAN 帧
结束
结束
结束
结束
结束
结束

图15

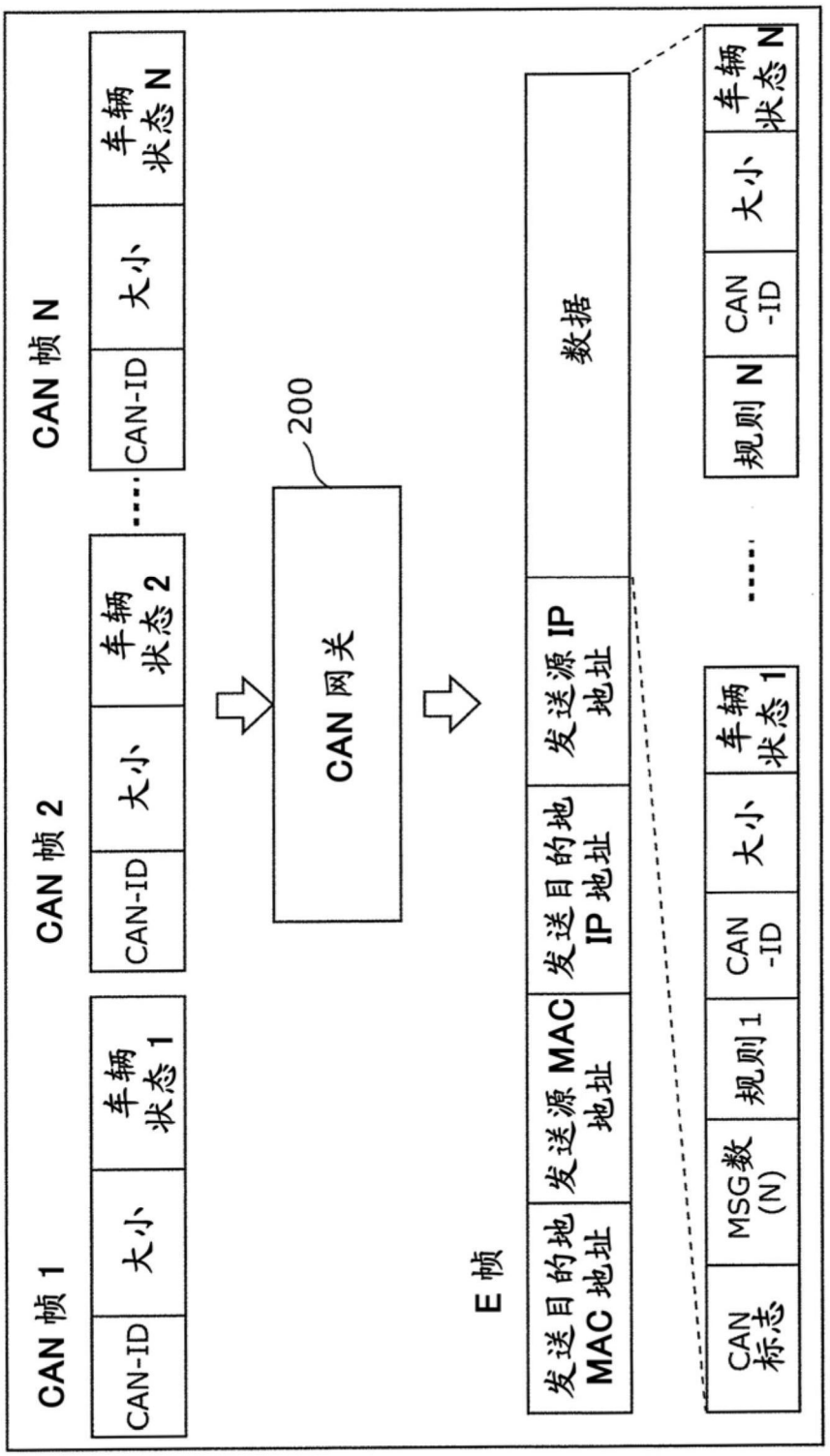

CAN 帧 1
CAN-ID
大小
车辆状态 1
CAN 帧 2
CAN-ID
大小
车辆状态 2
CAN 帧 N
CAN-ID
大小
车辆状态 N
200
CAN 网关
E 帧
发送目的地 MAC 地址
发送源 MAC 地址
发送目的地 IP 地址
发送源 IP 地址
数据
CAN 标志
MSG数 (N)
规则 1
CAN -ID
大小
车辆状态 1
规则 N
CAN -ID
大小
车辆状态 N

图16

规则 1	周期检查
规则 2	数据变化量检查
规则 3	MAC 检查

图17