



(12) 发明专利

(10) 授权公告号 CN 110406485 B

(45) 授权公告日 2023. 01. 06

(21) 申请号 201910660036.5

(22) 申请日 2015.03.23

(65) 同一申请的已公布的文献号
申请公布号 CN 110406485 A

(43) 申请公布日 2019.11.05

(30) 优先权数据
2015-032179 2015.02.20 JP
61/980,821 2014.04.17 US

(62) 分案原申请数据
201580002125.0 2015.03.23

(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

(72) 发明人 前田学 松岛秀树 芳贺智之
海上勇二 氏家良浩 岸川刚

(74) 专利代理机构 永新专利商标代理有限公司
72002

专利代理师 安香子

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

(56) 对比文件
US 2013073121 A1,2013.03.21
CN 103019759 A,2013.04.03
JP 2003271205 A,2003.09.26
JP H10107805 A,1998.04.24
JP 2013131907 A,2013.07.04

审查员 史文艳

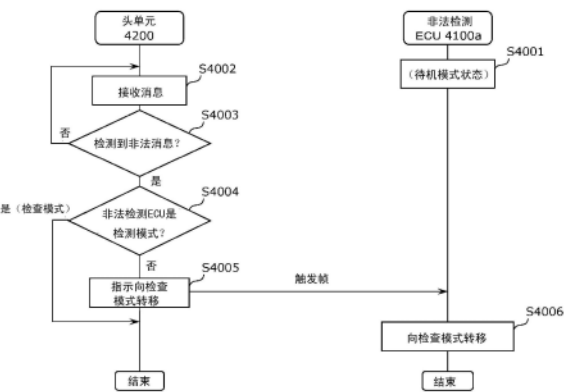
权利要求书2页 说明书34页 附图29页

(54) 发明名称

非法检测方法及车载网络系统

(57) 摘要

一种非法检测方法,在具备经由1个以上网络进行通信的多个电子控制单元的车载网络系统中使用,多个电子控制单元包括第1~第3电子控制单元;1个以上网络包括第1、第2网络;第1、第2电子控制单元分别连接于第1、第2网络;该方法包括:检测步骤,第3电子控制单元检测车辆的状态满足第1或第2条件的情况;及切换步骤,当满足上述第1或第2条件,则第3电子控制单元将切换指示消息发送给第1、第2电子控制单元,(i) 当满足第1条件,则第1、第2电子控制单元将动作模式转移到不进行检测1个以上网络上的非法消息的第1种处理的第1模式;(ii) 当满足第2条件,则第2电子控制单元将动作模式转移到进行第1种检测处理的第2模式。



1. 一种非法检测方法,在车载网络系统中使用,该车载网络系统具备经由1个以上的网络进行通信的多个电子控制单元,其中,

上述多个电子控制单元包括第1电子控制单元、第2电子控制单元以及第3电子控制单元;

上述1个以上的网络包括第1网络和第2网络;

上述第1电子控制单元连接于上述第1网络;

上述第2电子控制单元连接于上述第2网络;

上述非法检测方法包括:

检测步骤,上述第3电子控制单元检测具备上述车载网络系统的车辆的状态满足第1条件或第2条件的情况;以及

切换步骤,在检测到上述车辆的状态满足上述第1条件或上述第2条件的情况下,上述第3电子控制单元将切换指示消息发送给上述第1电子控制单元和上述第2电子控制单元,并且,

(i) 在检测到上述车辆的状态满足上述第1条件的情况下,上述第1电子控制单元和上述第2电子控制单元将动作模式转移到不进行第1种检测处理的第1模式,上述第1种检测处理是对上述1个以上的网络上的非法的消息进行检测的处理;

(ii) 在检测到上述车辆的状态满足上述第2条件的情况下,上述第2电子控制单元将动作模式转移到进行上述第1种检测处理的第2模式。

2. 如权利要求1所述的非法检测方法,其中,

上述第2条件是上述第3电子控制单元在上述1个以上的网络上检测到非法的消息。

3. 如权利要求2所述的非法检测方法,其中,

上述第1条件是上述第3电子控制单元在上述1个以上的网络上在规定的期间中没有检测到非法的消息。

4. 如权利要求1所述的非法检测方法,其中,

上述第2条件是上述第3电子控制单元成为开始与上述车辆的外部的装置进行通信的状态。

5. 如权利要求4所述的非法检测方法,其中,

上述第1条件是上述第3电子控制单元结束与上述车辆的外部的装置的通信而成为规定的状态。

6. 如权利要求1所述的非法检测方法,其中,

上述第2条件是上述车辆的状态为停车中。

7. 如权利要求6所述的非法检测方法,其中,

上述第2网络不包括上述多个电子控制单元之中的与上述车辆的驱动有关的电子控制单元。

8. 如权利要求1所述的非法检测方法,其中,

上述1个以上的网络还包括第3网络;

上述第3电子控制单元连接于上述第3网络;

上述车载网络系统还具备网关装置,该网关装置在上述第1网络、上述第2网络以及上述第3网络之间传送消息;

在上述切换步骤中，

上述第3电子控制单元将切换指示消息发送给上述网关装置；

在检测到上述车辆的状态满足上述第1条件的情况下，上述网关装置将上述切换指示消息发送给上述第1电子控制单元和上述第2电子控制单元；

在检测到上述车辆的状态满足上述第2条件的情况下，上述网关装置将上述切换指示消息发送给上述第2电子控制单元。

9. 如权利要求1所述的非法检测方法，其中，

上述第1条件或上述第2条件为，在上述车辆的状态变化的情况下，通过规定的用户接口受理表示需要上述动作模式的切换的输入。

10. 如权利要求1所述的非法检测方法，其中，

在上述第1模式中，进行能够检测非法的消息的程度与上述第1种检测处理不同的第2种检测处理。

11. 如权利要求1所述的非法检测方法，其中，

上述第3电子控制单元是在上述第1网络与上述第2网络之间传送消息的网关装置；

在上述切换步骤中，

在检测到上述车辆的状态满足上述第1条件的情况下，上述第3电子控制单元将上述切换指示消息发送给上述第1电子控制单元和上述第2电子控制单元；

在检测到上述车辆的状态满足上述第2条件的情况下，上述第3电子控制单元将上述切换指示消息发送给上述第2电子控制单元。

12. 如权利要求1所述的非法检测方法，其中，

上述多个电子控制单元按照控制器局域网协议即CAN协议，经由上述1个以上的网络进行通信。

13. 一种车载网络系统，其中，

具备经由1个以上的网络进行通信的多个电子控制单元；

上述多个电子控制单元包括第1电子控制单元、第2电子控制单元以及第3电子控制单元；

上述1个以上的网络包括第1网络和第2网络；

上述第1电子控制单元连接于上述第1网络；

上述第2电子控制单元连接于上述第2网络；

上述第3电子控制单元具备：

检测部，检测具备上述车载网络系统的车辆的状态满足第1条件或第2条件的情况；以及

发送部，在由上述检测部检测到上述车辆的状态满足上述第1条件或上述第2条件的情况下，将切换指示消息发送给上述第1电子控制单元和上述第2电子控制单元；

在检测到上述车辆的状态满足上述第1条件的情况下，上述第1电子控制单元和上述第2电子控制单元将动作模式转移到不进行第1种检测处理的第1模式，上述第1种检测处理是对上述1个以上的网络上的非法的消息进行检测的处理；

在检测到上述车辆的状态满足上述第2条件的情况下，上述第2电子控制单元将动作模式转移到进行上述第1种检测处理的第2模式。

非法检测方法及车载网络系统

[0001] 本申请是申请日为2015年3月23日、申请号为201580002125.0、发明名称为“车载网络系统、非法检测电子控制单元及非法检测方法”的发明专利申请的分案申请。

技术领域

[0002] 本发明涉及在电子控制单元进行通信的车载网络中对发送来的非法的帧进行检测的技术。

背景技术

[0003] 近年来,在汽车中的系统中,配置有许多称作电子控制单元(ECU:Electronic Control Unit)的装置。连接这些ECU的网络被称作车载网络。车载网络中存在许多的规格。其中最主流的车载网络之一中,存在由ISO11898-1规定的CAN(Controller Area Network:控制器局域网)的规格(参照“非专利文献1”)。

[0004] 在CAN中,通信路径由两条总线构成,连接于总线的ECU被称作节点。连接于总线的各节点对被称作帧的消息进行收发。发送帧的发送节点通过向两条总线施加电压、使得在总线之间产生电位差,来发送称作隐性(Recessive)的“1”的值、和称作显性(Dominant)的“0”的值。在多个发送节点以完全相同的定时发送了隐性和显性的情况下,显性被优先发送。接收节点在接受到的帧的格式中有异常的情况下,发送称作错误帧的帧。所谓错误帧,是通过将显性连续发送6bit而向发送节点、其他接收节点通知帧的异常的帧。

[0005] 此外,在CAN中,不存在指示发送目的地、发送源的识别码,发送节点按每个帧赋予称作消息ID的ID而发送(即向总线送出信号),各接收节点仅接收预先设定的消息ID(即从总线读取信号)。此外,采用CSMA/CA(Carrier Sense Multiple Access/Collision Avoidance)方式,在多节点的同时发送时进行基于消息ID的调解,消息ID的值较小的帧被优先发送。

[0006] 此外,已知有以下技术:在异常的消息被发送到CAN的总线上的情况下,由网关装置检测异常消息而不向其他总线转送,从而抑制总线的负荷上升(参照“专利文献1”)。

[0007] 现有技术文献

[0008] 专利文献

[0009] 专利文献1:特开2007-38904号公报

[0010] 非专利文献1:“CAN Specification 2.0Part A”,[online],CAN in Automation (CiA),[平成26年11月14日检索],因特网(URL:<http://www.can-cia.org/fileadmin/cia/specifications/CAN20A.pdf>)

[0011] 非专利文献2:RFC2104HMAC:Keyed-Hashing for Message Authentication

发明内容

[0012] 发明要解决的问题

[0013] 可是,在车载网络中,有可能将非法的节点连接到总线上、非法的节点非法地发送

帧(消息)从而非法地控制车体,所以为了抑制该情况,需要检测非法的消息。

[0014] 所以,本发明提供一种在按照CAN协议等进行通信的车载网络系统中、为了车载电池的消耗抑制等而有效率地检测向总线发送的非法的消息的非法检测电子控制单元(非法检测ECU)。此外,本发明提供用来有效地检测非法的消息的非法检测方法及具备非法检测ECU的车载网络系统。

[0015] 用于解决问题的手段

[0016] 有关本发明的一技术方案的非非法检测方法,在车载网络系统中使用,该车载网络系统具备经由1个以上的网络进行通信的多个电子控制单元,其中,上述多个电子控制单元包括第1电子控制单元、第2电子控制单元以及第3电子控制单元;上述1个以上的网络包括第1网络和第2网络;上述第1电子控制单元连接于上述第1网络;上述第2电子控制单元连接于上述第2网络;上述非法检测方法包括:检测步骤,上述第3电子控制单元检测具备上述车载网络系统的车辆的状态满足第1条件或第2条件的情况;以及切换步骤,在检测到上述车辆的状态满足上述第1条件或上述第2条件的情况下,上述第3电子控制单元将切换指示消息发送给上述第1电子控制单元和上述第2电子控制单元,(i)在检测到上述车辆的状态满足上述第1条件的情况下,上述第1电子控制单元和上述第2电子控制单元将动作模式转移到不进行第1种检测处理的第1模式,上述第1种检测处理是对上述1个以上的网络上的非法的消息进行检测的处理;(ii)在检测到上述车辆的状态满足上述第2条件的情况下,上述第2电子控制单元将动作模式转移到进行上述第1种检测处理的第2模式。

[0017] 此外,为了解决上述课题,有关本发明的一技术方案的车载网络系统,其中,具备经由1个以上的网络进行通信的多个电子控制单元;上述多个电子控制单元包括第1电子控制单元、第2电子控制单元以及第3电子控制单元;上述1个以上的网络包括第1网络和第2网络;上述第1电子控制单元连接于上述第1网络;上述第2电子控制单元连接于上述第2网络;上述第3电子控制单元具备:检测部,检测具备上述车载网络系统的车辆的状态满足第1条件或第2条件的情况;以及发送部,在由上述检测部检测到上述车辆的状态满足上述第1条件或上述第2条件的情况下,将切换指示消息发送给上述第1电子控制单元和上述第2电子控制单元;在检测到上述车辆的状态满足上述第1条件的情况下,上述第1电子控制单元和上述第2电子控制单元将动作模式转移到不进行第1种检测处理的第1模式,上述检测第1种处理是对上述1个以上的网络上的非法的消息进行检测的处理;在检测到上述车辆的状态满足上述第2条件的情况下,上述第2电子控制单元将动作模式转移到进行上述第1种检测处理的第2模式。

[0018] 此外,为了解决上述课题,有关本发明的一技术方案的非非法检测电子控制单元(非法检测ECU),是连接于经由1个以上的总线进行通信的多个电子控制单元在通信中使用的总线上的非法检测电子控制单元,具备:检测部,检测搭载上述车载网络系统的车辆的状态满足一定条件的情况;以及切换部,在由上述检测部检测到上述车辆的状态满足一定条件的情况下,将本装置的动作模式在第1模式与第2模式之间进行切换,该第1模式中进行对上述总线上的非法的消息进行检测的规定种类的检测处理,该第2模式不进行该规定种类的检测处理。

[0019] 发明效果

[0020] 根据本发明,例如在通过车载电池的电力等来工作的车载网络系统中,在非法的

节点连接到总线而发送了非法的消息的情况下能够进行其检测,并根据车辆的状态在一定条件下省略检测,所以能够抑制电池消耗。

附图说明

- [0021] 图1是表示有关实施方式1的车载网络系统的整体结构的图。
- [0022] 图2是表示由CAN协议规定的帧的格式的图。
- [0023] 图3是表示由CAN协议规定的错误帧的格式的图。
- [0024] 图4是头单元的结构图。
- [0025] 图5是表示接收ID列表的一例的图。
- [0026] 图6是网关的结构图。
- [0027] 图7是表示转送规则的一例的图。
- [0028] 图8是有关实施方式1的ECU的结构图。
- [0029] 图9是表示接收ID列表的一例的图。
- [0030] 图10是表示从与发动机连接的ECU发送的帧的ID及数据字段的一例的图。
- [0031] 图11是表示从与制动器连接的ECU发送的帧的ID及数据字段的一例的图。
- [0032] 图12是表示从与门开闭传感器连接的ECU发送的帧的ID及数据字段的一例的图。
- [0033] 图13是表示从与窗开闭传感器连接的ECU发送的帧的ID及数据字段的一例的图。
- [0034] 图14是表示有关实施方式1的非法检测ECU的结构图。
- [0035] 图15是表示非法检测ECU所保持的正规ID列表的一例的图。
- [0036] 图16是表示非法检测ECU所保持的正规ID列表的一例的图。
- [0037] 图17是表示各消息ID的非法检测计数器的状态的一例的图。
- [0038] 图18是表示实施方式1的有关非法的帧的检测及执行阻止的动作例的次序图。
- [0039] 图19是表示有关实施方式2的车载网络系统的整体结构的图。
- [0040] 图20是有关实施方式2的非法检测ECU的结构图。
- [0041] 图21是表示非法检测ECU所保持的数据范围列表的一例的图。
- [0042] 图22是表示实施方式2的有关非法的帧的检测及执行阻止的动作例的次序图(后接图23)。
- [0043] 图23是表示实施方式2的有关非法的帧的检测及执行阻止的动作例的次序图(前接图22)。
- [0044] 图24是表示有关实施方式3的车载网络系统的整体结构的图。
- [0045] 图25是表示有关实施方式3的ECU的结构图。
- [0046] 图26是表示从与发动机连接的ECU发送的数据帧的ID及数据字段的一例的图。
- [0047] 图27是表示从与制动器连接的ECU发送的数据帧的ID及数据字段的一例的图。
- [0048] 图28是表示从与门开闭传感器连接的ECU发送的数据帧的ID及数据字段的一例的图。
- [0049] 图29是表示从与窗开闭传感器连接的ECU发送的数据帧的ID及数据字段的一例的图。
- [0050] 图30是有关实施方式3的非法检测ECU的结构图。
- [0051] 图31是表示有关实施方式3的计数器保持部所保持的各消息ID的计数器值的一例

的图。

[0052] 图32是表示实施方式3的有关非法的帧的检测及执行阻止的动作例的次序图(后接图33)。

[0053] 图33是表示实施方式3的有关非法的帧的检测及执行阻止的动作例的次序图(前接图32)。

[0054] 图34是表示有关实施方式4的车载网络系统的整体结构的图。

[0055] 图35是有关实施方式4的头单元的结构图。

[0056] 图36是有关实施方式4的非法检测ECU的结构图。

[0057] 图37是表示实施方式4的向检查模式的转移次序的一例的图。

[0058] 图38是表示实施方式4的向待机模式的转移次序的一例的图。

[0059] 图39是表示实施方式4的向待机模式的转移次序的一例的图。

[0060] 图40是有关其他实施方式的ECU的结构图。

[0061] 图41是有关其他实施方式的非法检测ECU的结构图。

[0062] 图42是有关其他实施方式的非法检测ECU的结构图。

具体实施方式

[0063] 有关本发明的一技术方案的非法检测方法,在具备经由1个以上的总线进行通信的多个电子控制单元的车载网络系统中使用,包括:检测步骤,检测搭载上述车载网络系统的车辆的状态满足一定条件的情况;以及切换步骤,在上述检测步骤中检测到上述车辆的状态满足一定条件的情况下,将连接于上述总线的非法检测电子控制单元的动作模式在第1模式与第2模式之间进行切换,该第1模式中进行对该总线上的非法的消息进行检测的规定种类的检测处理,该第2模式中不进行该规定种类的检测处理。这里,非法检测电子控制单元(非法检测ECU)连接于总线,具有执行用来检测发送到该总线的非法的消息的规定种类的检测处理的功能。是否是非法的消息,由检测处理根据是否适合预先决定的条件来判断。例如在非法检测ECU仅进行1种检测处理的情况下,通过动作模式切换是否进行检测处理。根据该非法检测方法,根据车辆的状态,在一定条件下非法检测ECU能够省略非法的消息的规定种类的检测处理,所以能够抑制车辆的电池消耗。

[0064] 此外,也可以是,上述多个多个电子控制单元按照Controller Area Network (CAN) 协议经由上述总线进行通信。由此,可以根据车辆的状态来限定在非法的ECU连接到按照CAN协议进行通信的车载网络系统上而发送了非法的帧的情况下非法检测ECU检测该非法的期间,所以能够降低电力消耗量。

[0065] 此外,也可以是,在上述检测步骤中,作为上述多个电子控制单元中的1个电子控制单元进行上述检测;在上述切换步骤中,在上述检测步骤中进行了上述检测的1个电子控制单元发送切换指示消息,在接收到该切换指示消息的情况下,上述非法检测电子控制单元将上述动作模式切换。由此,例如,非法检测ECU在不进行检测非法的消息的检测处理的第2模式中,仅进行切换指示消息(即作为动作模式的切换的触发的触发帧)的检测就足够。即,非法检测ECU也可以不具有用来直接检测车辆的状态的检测部(例如传感器等)。

[0066] 此外,也可以是,在上述检测步骤中,在上述1个电子控制单元在上述总线上检测到非法的消息的情况下,视为上述车辆的状态满足上述一定条件而进行上述检测;在上述

切换步骤中,在上述检测步骤中进行了上述检测的情况下,上述1个电子控制单元发送表示切换为上述第1模式的切换指示消息,在接收到该切换指示消息的情况下,上述非法检测电子控制单元将上述动作模式切换为上述第1模式。由此,在检测到在某个总线上被发送了非法的消息的情况下,非法检测ECU成为第1模式(检测非法的消息的检查模式),检测与非法检测ECU连接的总线上的非法的消息。

[0067] 此外,也可以是,在上述检测步骤中,在上述1个电子控制单元在上述总线上在一定期间中没有检测到非法的消息的情况下,视为上述车辆的状态满足上述一定条件而进行上述检测;在上述切换步骤中,在上述检测步骤中进行了上述检测的情况下,上述1个电子控制单元发送表示切换为上述第2模式的切换指示消息,在接收到该切换指示消息的情况下,上述非法检测电子控制单元将上述动作模式切换为上述第2模式。由此,在检测到在某个总线上在一定期间中没有被发送非法的消息的情况下,非法检测ECU成为第2模式(不检测非法的消息的待机模式),能够降低电力消耗量。

[0068] 此外,也可以是,上述一定条件是开始了上述车辆的使用;在上述切换步骤中,在上述检测步骤中检测到开始了上述车辆的使用的情况下,将上述动作模式切换为上述第1模式。所谓车辆的使用,例如是用户使车辆行驶、进行车辆的行驶的准备(开门、乘车、发动机启动等)。此外,例如在不需要行驶时,通过停车(发动机停止等)、下车等而使用结束。另外也可以是,在用户的自宅的停车场等特定的停车场以外的场所的停车中(加油站或其他外出地的停车中)中,即使有停车及下车也作为使用没有结束来处理。由此,在开始了车辆的使用的情况下,非法检测ECU成为第1模式(检测非法的消息的检查模式),与非法检测ECU连接的总线上的非法的消息被检测出。因而,即使例如在停车而用户离开车辆的期间中车载网络系统被附加了非法的ECU,也从用户回到车辆而开始车辆的使用起,如果该非法的ECU发送非法的消息,则能够检测到该非法。

[0069] 此外,也可以是,通过检测搭载在上述车辆中的发动机启动的情况,来进行开始了车辆的使用的情况的上述检测。由此,从发动机启动时起,成为非法检测ECU检测非法的消息的状态。因而,即使例如在停车而用户离开车辆的期间中车载网络系统被附加了非法的ECU,也从用户回到车辆而开始车辆的使用起,如果该非法的ECU发送非法的消息,则能够检测到该非法。

[0070] 此外,也可以是,上述非法检测方法还包括再切换步骤,在上述再切换步骤中上述动作模式被切换为上述第1模式后,从开始上述车辆的使用起经过了规定时间时,将上述动作模式切换为上述第2模式。由此,在从开始车辆的使用起经过了规定时间时,无条件或在一定条件下非法检测ECU成为第2模式(不检测非法的消息的待机模式),能够降低电力消耗量。

[0071] 此外,也可以是,上述一定条件是上述多个电子控制单元中的某一个成为了与上述车辆的外部的装置开始通信的状态;在上述切换步骤中,在上述检测步骤中检测到成为了开始上述通信的状态的情况下,将上述动作模式切换为上述第1模式。由此,如果开始与外部的通信,则非法检测ECU成为检测非法的消息的状态。因而,即使例如从外部的装置攻击车载网络系统的头单元等、而从外部注入非法的消息(帧),也能够迅速地检测到。另外,在从外部供给了用来发送非法的消息的程序等那样的情况下也能够同样地应对。

[0072] 此外,上述一定条件是上述多个电子控制单元中的某一个与上述车辆的外部的装

置进行通信并成为了通信结束后的一定状态;在上述切换步骤中,在上述检测步骤中检测到成为了上述通信结束后的一定状态的情况下,将上述动作模式切换为上述第2模式。由此,在与外部的通信结束从而非法的消息发送到总线上的可能性下降的情况下,通过省略非法的消息的检测,能够抑制电池消耗。另外,发送非法的消息的可能性下降的情况,具体而言,例如是成为通信被切断的状态的情况、从通信结束起经过了一定时间(例如几分钟)的状态的情况等。

[0073] 此外,也可以是,在上述车载网络系统中,在上述多个电子控制单元的通信中使用多个总线;上述车载网络系统还具备网关装置,该网关装置具有在上述多个总线之间转送消息的功能;在上述检测步骤中,上述多个电子控制单元中的连接于与上述非法检测电子控制单元不同的总线上的1个电子控制单元进行上述检测;在上述切换步骤中,在上述检测步骤中进行了上述检测的1个电子控制单元发送切换指示消息,在接收到转送给上述网关装置的该切换指示消息的情况下上述非法检测电子控制单元将上述动作模式切换。由此,根据由车载网络系统中的连接于1个总线的ECU检测到的车辆的状态,分别连接于其他1个以上的总线的各非法检测ECU能够切换动作模式。

[0074] 此外,也可以是,在上述检测步骤中,在车辆的状态变化的情况下,通过规定的用户接口受理与是否需要上述动作模式的切换有关的输入,当该输入表示需要上述动作模式的切换时,视为上述车辆的状态满足上述一定条件而进行上述检测。由此,由于用户的判断被反映到非法检测ECU的动作模式的切换中,所以根据用户的情况等适当地切换动作模式。

[0075] 此外,也可以是,在上述第2模式中,进行能够检测非法的消息的程度与上述规定种类的检测处理不同的种类的检测处理。例如在非法检测ECU为了检测非法的消息而能够执行处理量比较多的第一种检测处理和处理量比较少的第二种检测处理的情况下,通过动作模式切换是进行第一种检测处理还是进行第二种检测处理。由此,根据车辆的状态,在一定条件下,非法检测ECU能够将非法的消息的规定种类的检测处理(例如第一种检测处理)省略,所以能够抑制车辆的电池消耗。另外,非法检测ECU中的检测处理的处理量的多少并不一定与能够检测非法的程度的高低成比例,但是有大致与能够检测非法的消息的程度的高低关联的趋向。因此,例如大致以仅限于一定的情况执行非法检测程度较高且处理量较多的检测处理、在其他情况下进行处理量比其少的检测处理的方式切换动作模式等变得有用。

[0076] 此外,有关本发明的一技术方案的车载网络系统,是具备经由1个以上的总线进行通信的多个电子控制单元、和连接于上述总线的非法检测电子控制单元的车载网络系统,具备:检测部,检测搭载上述车载网络系统的车辆的状态满足一定条件的情况;以及切换部,在由上述检测部检测到上述车辆的状态满足一定条件的情况下,将连接于上述总线的非法检测电子控制单元的动作模式在第1模式与第2模式之间进行切换,该第1模式中进行对该总线上的非法的消息进行检测的规定种类的检测处理,该第2模式中不进行该规定种类的检测处理。由此,根据车辆的状态,在一定条件下,非法检测ECU能够将非法的消息的规定种类的检测处理省略,所以能够抑制车辆的电池消耗。

[0077] 此外,有关本发明的一技术方案的非非法检测电子控制单元(非法检测ECU),连接于经由1个以上的总线进行通信的多个电子控制单元在通信中使用的总线,具备:检测部,检测搭载上述多个电子控制单元的车辆的状态满足一定条件的情况;以及切换部,在由上述

检测部检测到上述车辆的状态满足一定条件的情况下,将本装置的动作模式在第1模式与第2模式之间进行切换,该第1模式中进行对上述总线上的非法的消息进行检测的规定种类的检测处理,该第2模式中不进行该规定种类的检测处理。由此,根据车辆的状态,在一定条件下,非法检测ECU能够将非法的消息的规定种类的检测处理省略,所以能够抑制车辆的电池消耗。

[0078] 另外,这些整体性或具体的技术方案既可以通过系统、方法、集成电路、计算机程序或计算机可读的CD-ROM等记录介质实现,也可以通过系统、方法、集成电路、计算机程序及记录介质的任意的组合实现。

[0079] 以下,参照附图对有关实施方式的车载网络系统、非法检测ECU等进行说明。这里所示的实施方式都表示本发明的一具体例。因而,在以下的实施方式中表示的数值、形状、材料、构成要素、构成要素的配置位置及连接形态、步骤(工序)及步骤的顺序等是一例,并不限定本发明。以下的实施方式的构成要素中的、在独立权利要求中没有记载的构成要素,是可任意地附加的构成要素。此外,各图是示意图,并不是严格地图示的。

[0080] (实施方式1)

[0081] 以下,作为本发明的实施方式,使用附图说明包括非法检测ECU的车载网络系统10,该非法检测ECU使用消息ID实现用来阻止在其他节点(ECU)中执行基于非法的帧的处理的非法应对方法。

[0082] [1.1车载网络系统10的整体结构]

[0083] 图1是表示有关实施方式1的车载网络系统10的整体结构的图。车载网络系统10是按照CAN协议进行通信的网络通信系统的一例,是搭载有控制装置、传感器等各种设备的汽车的网络通信系统。车载网络系统10构成为包括总线500a、500b、和非法检测ECU100a、100b、头单元200、网关300及与各种设备连接的ECU400a~400d等ECU这样的连接于总线的各节点。另外,虽然在图1中省略了,但在车载网络系统10中除了ECU400a~400d以外还可以包括一些ECU,这里,为了方便而关注于ECU400a~400d进行说明。ECU例如是包括处理器(微处理器)、存储器等数字电路、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控制程序(计算机程序)。例如通过由处理器按照控制程序(计算机程序)动作,ECU实现各种功能。另外,计算机程序是为了达到规定的功能而将表示对于处理器的指令的命令代码组合多个而构成的。这里,以在总线500a、500b上有可能连接着发送非法的帧的非法ECU为前提进行说明。

[0084] 非法检测ECU100a、100b分别连接于总线500a、总线500b,是具有判定由ECU400a~400d等发送的帧是否是非法的、如果是非法则发送错误帧的功能的ECU。

[0085] ECU400a~400d与某个总线连接,此外,分别连接于发动机401、制动器402、门开闭传感器403、窗开闭传感器404。ECU400a~400d分别取得所连接的设备(发动机401等)的状态,定期地向网络(即总线)发送表示状态的帧(后述的数据帧)等。

[0086] 网关300连接于与非法检测ECU100a、ECU400a及ECU400b连接的总线500a、与非法检测ECU100b、ECU400c及ECU400d连接的总线500b、以及与头单元200连接的总线500c,具有将从各个总线接收到的帧向其他总线转送的功能。此外,也可以按每个所连接的总线间来切换是否将接收到的帧转送。网关300也是一种ECU。

[0087] 头单元200具有接收帧的功能,具有接收从ECU400a~400d发送的帧、将各种状态

显示在显示器(未图示)上、向用户提示的功能。头单元200也是一种ECU。

[0088] 在该车载网络系统10中,各ECU按照CAN协议进行帧的交换。CAN协议的帧中,有数据帧、远程帧、过载帧及错误帧。为了说明的方便,首先以数据帧及错误帧为中心进行说明。

[0089] [1.2数据帧格式]

[0090] 以下,对作为遵循CAN协议的网络中使用的帧之一的数据帧进行说明。

[0091] 图2是表示由CAN协议规定的帧的格式的图。在该图中,表示由CAN协议规定的标准ID格式中的数据帧。数据帧由SOF (Start Of Frame)、ID字段、RTR (Remote Transmission Request)、IDE (Identifier Extension)、保留位“r”、DLC (Data Length Code)、数据字段、CRC (Cyclic Redundancy Check) 序列、CRC定界符“DEL”、ACK (Acknowledgement) 时隙、ACK定界符“DEL”及EOF (End Of Frame) 的各字段构成。

[0092] SOF由1bit的显性构成。总线是空闲的状态为隐性,通过SOF向显性变更从而通知帧的发送开始。

[0093] ID字段是由11bit构成的、将作为表示数据的种类的值的ID (消息ID) 进行保存的字段。在多个节点同时开始发送的情况下,为了用该ID字段进行通信调解,设计为使ID具有较小值的帧为较高的优先级。

[0094] RTR是用来识别数据帧和远程帧的值,在数据帧中由显性1bit构成。

[0095] IDE和“r”两者都由显性1bit构成。

[0096] DLC由4bit构成,是表示数据字段的长度的值。另外,将IDE、“r”及DLC一起称作控制字段。

[0097] 数据字段是最大由64bit构成的表示所发送的数据的内容的值。能够按每8bit调整长度。关于发送的数据的规格,没有由CAN协议规定,而在车载网络系统10中设定。所以是依赖于车种、制造者(制造厂商)等的规格。

[0098] CRC序列由15bit构成。根据SOF、ID字段、控制字段及数据字段的发送值计算。

[0099] CRC定界符是由1bit的隐性构成的表示CRC序列的结束的分隔符号。另外,将CRC序列及CRC定界符一起称作CRC字段。

[0100] ACK时隙由1bit构成。发送节点使ACK时隙为隐性而进行发送。接收节点如果正常地接收到CRC序列为止,则将ACK时隙设为显性而发送。由于显性比隐性优先,所以如果在发送后ACK时隙是显性,则发送节点能够确认到某个接收节点接收成功。

[0101] ACK定界符是由1bit的隐性构成的表示ACK的结束的分隔符号。

[0102] EOF由7bit的隐性构成,表示数据帧的结束。

[0103] [1.3错误帧格式]

[0104] 图3是表示由CAN协议规定的错误帧的格式的图。错误帧由错误标志(主)、错误标志(副)和错误定界符构成。

[0105] 错误标志(主)用于向其他节点通知错误的发生。检测到错误的节点为了向其他节点通知错误的发生,将6bit的显性连续地发送。该发送违反CAN协议中的位填充规则(不将相同的值连续发送6bit以上),引起从其他节点的错误帧(副)的发送。

[0106] 错误标志(副)由为了将错误的发生向其他节点通知而使用的连续的6位的显性构成。接收错误标志(主)而检测到违反位填充规则的全部的节点发送错误标志(副)。

[0107] 错误定界符“DEL”是8bit的连续的隐性,表示错误帧的结束。

[0108] [1.4头单元200的结构]

[0109] 头单元200例如设置于汽车的仪表板(instrument panel)等,是具备显示用来由驾驶者视觉辨识的信息的液晶显示器(LCD:liquid crystal display)等显示装置、受理驾驶者的操作的输入机构等的一种ECU。

[0110] 图4是头单元200的结构图。头单元200构成为包括帧收发部270、帧解释部260、接收ID判断部240、接收ID列表保持部250、帧处理部220、显示控制部210和帧生成部230。这些各构成要素是功能性的构成要素,其各功能通过头单元200的通信电路、LCD、执行保存在存储器中的控制程序的处理器或数字电路等实现。

[0111] 帧收发部270对于总线500c收发遵循CAN协议的帧。从总线500c每次1bit地接收帧,向帧解释部260转送。此外,将从帧生成部230接受到通知的帧的内容向总线500c每次1bit地发送。

[0112] 帧解释部260从帧收发部270获取帧的值,进行解释,以映射到由CAN协议规定的帧格式的各字段。帧解释部260将判断为ID字段的值向接收ID判断部240转送。帧解释部260根据从接收ID判断部240通知的判定结果,决定是将ID字段的值和ID字段以后出现的数据字段向帧处理部220转送、还是在接受到该判定结果以后将帧的接收中止(即,将作为该帧的解释中止)。此外,帧解释部260例如在CRC的值不一致、或显性固定的项目是隐性等、判断为不符合CAN协议的帧的情况下,向帧生成部230通知以使其发送错误帧。此外,帧解释部260在接收到错误帧的情况下,即在根据接收到的帧的值解释为错误帧的情况下,其以后将该帧丢弃,即中止帧的解释。例如在从数据帧的中途被解释为错误帧的情况下,该数据帧的解释被中止,不再根据该数据帧进行特别的处理。

[0113] 接收ID判断部240接受从帧解释部260通知的ID字段的值,按照接收ID列表保持部250保持的消息ID的列表,进行是否接收该ID字段以后的帧的各字段的判定。接收ID判断部240将该判定结果向帧解释部260通知。

[0114] 接收ID列表保持部250保持头单元200接收的ID(消息ID)的列表即接收ID列表。图5是表示接收ID列表的一例的图。头单元200从与发动机401连接的ECU400a接收消息ID是“1”的帧(消息),从与制动器402连接的ECU400b接收消息ID是“2”的帧,从与门开闭传感器403连接的ECU400c接收消息ID是“3”的帧,从与窗开闭传感器404连接的ECU400d接收消息ID是“4”的帧。

[0115] 帧处理部220基于接收到的帧的内容(例如消息ID及数据字段的内容),形成例如要向LCD显示的图像,向显示控制部210通知。另外,帧处理部220也可以将接收到的数据字段的内容进行保持,按照通过输入机构受理的驾驶者的操作,选择要向LCD显示的图像(例如车速显示用的图像、窗开闭状态显示用的图像等)并通知。

[0116] 显示控制部210将从帧处理部220接受到通知的内容向LCD等显示。

[0117] 帧生成部230按照来自帧解释部260的、指示错误帧的发送的通知,构成错误帧,将错误帧向帧收发部270通知而使其发送。

[0118] [1.5接收ID列表例1]

[0119] 图5是表示在头单元200、网关300、ECU400c及ECU400d的各自中保持的接收ID列表的一例的图。该图所例示的接收ID列表用于将包含ID(消息ID)的值是“1”、“2”、“3”及“4”中的某一个的消息ID的帧有选择地接收并处理。例如,如果在头单元200的接收ID列表保持部

250中保持着图5的接收ID列表,则关于消息ID不是“1”、“2”、“3”及“4”中的任何一个的帧,将帧解释部260中的ID字段以后的帧的解释中止。

[0120] [1.6网关300的结构]

[0121] 图6是网关300的结构图。网关300构成为包括帧收发部360、帧解释部350、接收ID判断部330、接收ID列表保持部340、帧生成部320、转送处理部310和转送规则保持部370。这些各构成要素是功能性的构成要素,其各功能由网关300中的通信电路、执行保存在存储器中的控制程序的处理器或数字电路等实现。

[0122] 帧收发部360对于总线500a、500b、500c分别收发遵循CAN协议的帧。从总线将帧每次1bit地接收,向帧解释部350转送。此外,基于表示从帧生成部320接受到通知的转送目的地的总线的总线信息及帧,将该帧的内容向总线500a、500b、500c每次1bit地发送。

[0123] 帧解释部350从帧收发部360接受帧的值,进行解释以映射到由CAN协议规定的帧格式的各字段。将判断为ID字段的值向接收ID判断部330转送。帧解释部350根据从接收ID判断部330通知的判定结果,决定是将ID字段的值和ID字段以后出现的数据字段(数据)向转送处理部310转送、还是在接受到该判定结果以后将帧的接收中止(即,将作为该帧的解释中止)。此外,帧解释部350在判断为不符合CAN协议的帧的情况下,向帧生成部320通知以使其发送错误帧。此外,帧解释部350在接收到错误帧的情况下,即在根据接受到的帧中的值解释为错误帧的情况下,在其以后将该帧丢弃,即中止帧的解释。

[0124] 接收ID判断部330接受从帧解释部350通知的ID字段的值,按照接收ID列表保持部340保持的消息ID的列表,进行是否接收该ID字段以后的帧的各字段的判定。接收ID判断部330将该判定结果向帧解释部350通知。

[0125] 接收ID列表保持部340保持网关300接收的ID(消息ID)的列表即接收ID列表(参照图5)。

[0126] 转送处理部310按照转送规则保持部370保持的转送规则,根据接收到的帧的消息ID决定转送的总线,将表示转送的总线的总线信息、由帧解释部350通知的消息ID和数据向帧生成部320通知。另外,网关300关于从某个总线接收到的错误帧,不向其他总线转送。

[0127] 转送规则保持部370保持表示关于各总线的帧的转送的规则的信息即转送规则。图7是表示转送规则的一例的图。

[0128] 帧生成部320按照由帧解释部350通知的、指示错误帧的发送的通知,构成错误帧,将错误帧向帧收发部360通知而使其发送。此外,帧生成部320使用由转送处理部310通知的消息ID和数据构成帧,将帧及总线信息向帧收发部360通知。

[0129] [1.7转送规则例]

[0130] 图7表示网关300拥有的转送规则的一例。该转送规则中将转送源总线、转送目的地总线和转送对象ID(消息ID)建立了对应。图7中的“*”表示不论消息ID如何都进行帧的转送。此外,该图中的“—”表示没有转送对象帧。该图的例子表示设定为,从总线500a接收的帧不论消息ID如何都向总线500b及总线500c转送。此外,表示设定为,从总线500b接收的帧中,向总线500c转送全部的帧,而向总线500a仅转送消息ID是“3”的帧。此外,表示设定为,从总线500c接收的帧既不向总线500a转送也不向总线500b转送。

[0131] [1.8ECU400a的结构]

[0132] 图8是ECU400a的结构图。ECU400a构成为包括帧收发部460、帧解释部450、接收ID

判断部430、接收ID列表保持部440、帧处理部410、帧生成部420和数据取得部470。这些各构成要素是功能性的构成要素,其各功能通过ECU400a中的通信电路、执行保存在存储器中的控制程序的处理器或数字电路等实现。

[0133] 帧收发部460对于总线500a收发遵循CAN协议的帧。从总线500a将帧每次1bit地接收,向帧解释部450转送。此外,将从帧生成部420接受到通知的帧的内容向总线500a发送。

[0134] 帧解释部450从帧收发部460接受帧的值,进行解释以映射到由CAN协议规定的帧格式的各字段。将判断为ID字段的值向接收ID判断部430转送。帧解释部450根据由接收ID判断部430通知的判定结果,决定是将ID字段的值和ID字段以后出现的数据字段向帧处理部410转送、还是在接受到该判定结果以后将帧的接收中止(即,将作为该帧的解释中止)。此外,帧解释部450在判断为不符合CAN协议的帧的情况下,向帧生成部420通知以使其发送错误帧。此外,帧解释部450在接收到错误帧的情况下,即在根据接受到的帧中的值解释为错误帧的情况下,在其以后将该帧丢弃,即中止帧的解释。

[0135] 接收ID判断部430接受由帧解释部450通知的ID字段的值,按照接收ID列表保持部440保持的消息ID的列表,进行是否接收该ID字段以后的帧的各字段的判定。接收ID判断部430将该判定结果向帧解释部450通知。

[0136] 接收ID列表保持部440保持ECU400a接收的ID(消息ID)的列表即接收ID列表。图9是表示接收ID列表的一例的图。

[0137] 帧处理部410根据接收到的帧的数据进行与按每个ECU而不同的功能有关的处理。例如,连接于发动机401的ECU400a具备如果是在时速超过30km的状态下门打开的状态则鸣响警报音的功能。ECU400a具有用来鸣响例如警报音的扬声器等。并且,ECU400a的帧处理部410管理从其他ECU接收到的数据(例如表示门的状态的信息),进行基于从发动机401取得的时速在一定条件下鸣响警报音的处理等。

[0138] 数据取得部470取得表示连接于ECU的设备、传感器等的状态的数据,向帧生成部420通知。

[0139] 帧生成部420按照由帧解释部450通知的指示错误帧的发送的通知,构成错误帧,将错误帧向帧收发部460通知而使其发送。此外,帧生成部420对于由数据取得部470通知的数据的值赋予预先决定的消息ID而构成帧,向帧收发部460通知。

[0140] 另外,ECU400b~400d也具备基本上与上述ECU400a同样的结构。但是,保持在接收ID列表保持部440中的接收ID列表的内容可以按每个ECU而不同。ECU400b保持图9所例示的接收ID列表,ECU400c及ECU400d保持图5所例示的接收ID列表。此外,帧处理部410的处理内容按每个ECU而不同。例如,ECU400c的帧处理部410的处理内容包括有关如果在没有施加制动的状况下门打开则鸣响警报音的功能的处理。例如,在ECU400b及ECU400d的帧处理部410中不进行特别的处理。另外,各ECU也可以具备这里例示的以外的功能。另外,关于ECU400a~400d分别发送的帧的内容在后面使用图10~图13说明。

[0141] [1.9接收ID列表例2]

[0142] 图9是表示在ECU400a及ECU400b的各自中保持的接收ID列表的一例的图。该图所例示的接收ID列表用于将包含ID(消息ID)的值是“1”,“2”及“3”中的任一个的消息ID的帧有选择地接收并处理。例如,如果在ECU400a的接收ID列表保持部440中保持着图9的接收ID列表,则关于消息ID不是“1”、“2”及“3”的任何一个的帧,将帧解释部450中的ID字段以后的

帧的解释中止。

[0143] [1.10有关发动机的ECU400a的发送帧例]

[0144] 图10是表示从与发动机401连接的ECU400a发送的帧的ID(消息ID)及数据字段(数据)的一例的图。ECU400a发送的帧的消息ID是“1”。数据表示时速(km/时),取最低0(km/时)~最高180(km/时)的范围的值,数据长是1byte。从图10的上行向下行,例示了与从ECU400a依次发送的各帧对应的各消息ID及数据,表示从0km/时起每加速1km/时的情形。

[0145] [1.11有关制动器的ECU400b的发送帧例]

[0146] 图11是表示从与制动器402连接的ECU400b发送的帧的ID(消息ID)及数据字段(数据)的一例的图。ECU400b发送的帧的消息ID是“2”。关于数据,用比例(%)表示制动的施加状况,数据长是1byte。该比例是设完全没有施加制动的状态为0(%)、设最大限度施加了制动的状态为100(%)的比例。从图11的上行向下行,例示了与从ECU400b依次发送的各帧对应的各消息ID及数据,表示从100%起逐渐将制动减弱的情形。

[0147] [1.12有关门开闭传感器的ECU400c的发送帧例]

[0148] 图12是表示从与门开闭传感器403连接的ECU400c发送的帧的ID(消息ID)及数据字段(数据)的一例的图。ECU400c发送的帧的消息ID是“3”。数据表示门的开闭状态,数据长是1byte。对数据的值而言,门打开的状态是“1”,门关闭的状态是“0”。从图12的上行向下行,例示了与从ECU400c依次发送的各帧对应的各消息ID及数据,表示门从打开的状态起逐渐向关闭的状态转移的情形。

[0149] [1.13有关窗开闭传感器的ECU400d的发送帧例]

[0150] 图13是表示从与窗开闭传感器404连接的ECU400d发送的帧的ID(消息ID)及数据字段(数据)的一例的图。ECU400d发送的帧的消息ID是“4”。数据将窗的开闭状态用比例(%)表示,数据长是1byte。该比例是设窗完全关闭的状态为0(%)、设窗全开的状态为100(%)的比例。从图13的上行向下行,例示了与从ECU400d依次发送的各帧对应的各消息ID及数据,表示窗从关闭的状态逐渐打开的情形。

[0151] [1.14非法检测ECU100a的结构]

[0152] 图14是非法检测ECU100a的结构图。非法检测ECU100a构成为包括帧收发部160、帧解释部150、非法帧检测部130、正规ID列表保持部120、非法检测计数器保持部110和帧生成部140。这些各构成要素是功能性的构成要素,其各功能由非法检测ECU100a中的通信电路、执行保存在存储器中的控制程序的处理器或数字电路等实现。另外,非法检测ECU100b也基本上具备同样的结构,但正规ID列表保持部120保持的列表信息(正规ID列表)的内容在非法检测ECU100a和非法检测ECU100b中不同。

[0153] 帧收发部160对于总线500a收发遵循CAN协议的帧。即,帧收发部160作为在开始了总线上的帧的发送的情况下接收帧的所谓接收部发挥作用,此外作为向总线发送错误帧等的所谓发送部发挥作用。即,帧收发部160从总线500a将帧每次1bit地接收,向帧解释部150转送。此外,将从帧生成部140接受到通知的帧的内容向总线500a发送。

[0154] 帧解释部150从帧收发部160接受帧的值,进行解释以映射到由CAN协议规定的帧格式的各字段。将判断为ID字段的值向非法帧检测部130转送。此外,帧解释部150在判断为不符合CAN协议的帧的情况下,向帧生成部140通知以使其发送错误帧。此外,帧解释部150在接收到错误帧的情况下,即在根据接受到的帧中的值解释为错误帧的情况下,在其以后

将该帧丢弃,即中止帧的解释。

[0155] 非法帧检测部130接受由帧解释部150通知的ID字段的值,判定ID字段的值是否与表示非法的规定条件相符。即,非法帧检测部130作为判定接收到的帧中的规定字段的内容是否与表示非法的规定条件相符的所谓判定部发挥功能。该表示非法的规定条件是ID字段的值没有记载在正规ID列表保持部120保持的消息ID的列表中的条件。即,按照正规ID列表保持部120保持的消息ID的列表,进行被通知的ID字段的值(消息ID)是否非法的判定。在接收到没有记载在该列表(即后述的正规ID列表)中的消息ID的情况下,为了将非法的检测次数递增,将接收到的消息ID向非法检测计数器保持部110通知。此外,在接收到没有记载在正规ID列表中的消息ID的情况下,向帧生成部140通知以使其发送错误帧。此外,在非法的检测次数达到一定次数以上的情况下,从非法检测计数器保持部110接受通知,向帧生成部140通知,以使其发送表示存在发行相应的消息ID的非法的ECU的错误显示消息(帧)。错误显示消息的消息ID被预先决定,头单元200接收该消息ID的消息(帧)而进行错误显示。关于该错误显示消息,为了方便而省略了说明,但错误显示消息的消息ID登载在网关300及头单元200保持的接收ID列表及后述的正规ID列表中。但是,在图15、图16中省略了关于错误显示消息的消息ID。

[0156] 正规ID列表保持部120保持正规ID列表,该正规ID列表是预先规定了在车载网络系统10中在总线500a上发送的帧中包含的消息ID的列表(参照图15、图16)。

[0157] 非法检测计数器保持部110保持着用来按每个消息ID将检测次数进行计数的非法检测计数器,如果被从非法帧检测部130通知消息ID,则将相应的非法检测计数器递增(增加)。在非法检测计数器达到了一定数量(规定次数)以上的情况下,向非法帧检测部130通知超过了一定数量。这里所述一定数量(规定次数)的一例是与CAN协议中的发送错误计数器的处理规则对应地设定的值。在CAN协议中,每当ECU通过错误帧阻止发送,则发送错误计数器计数增加8。并且规定:如果作为其结果而发送节点中的发送错误计数器计数增加到128,则发送节点转移为被动状态而不再进行帧发送。因而,如果将比 $128/8 (=16)$ 大的17设定为该一定数量,则在推测为存在忽视了CAN协议中的有关发送错误计数器的规则的发送节点(非法的ECU)的情况下,从非法检测ECU100a发送错误显示消息。另外,在发送非法的帧的非法的ECU是遵循CAN协议中的有关发送错误计数器的规则的ECU的情况下,通过由非法检测ECU100a发送错误帧,非法的ECU的发送错误计数器被递增8。在此情况下,如果通过重复非法的帧的发送而非法的ECU的发送错误计数器上升到128,则非法的ECU转移为被动状态,由非法的ECU进行的非法的帧的发送停止。

[0158] 帧生成部140按照由帧解释部150通知的、指示错误帧的发送的通知,构成错误帧,将错误帧向帧收发部160通知而使其发送。此外,帧生成部140按照由非法帧检测部130通知的、指示错误帧的发送的通知,构成错误帧,将错误帧向帧收发部160通知而使其发送。进而,帧生成部140按照由非法帧检测部130通知的、指示错误显示消息的发送的通知,将错误显示消息向帧收发部160通知而使其发送。

[0159] [1.15非法检测ECU100a的正规ID列表例]

[0160] 图15是表示在非法检测ECU100a的正规ID列表保持部120中保持的正规ID列表的一例的图。该图所例示的正规ID列表表示包含ID(消息ID)的值是“1”、“2”及“3”中的某一个的消息ID的帧能够流到总线500a中。

[0161] [1.16非法检测ECU100b的正规ID列表例]

[0162] 图16是表示在非法检测ECU100b的正规ID列表保持部120中保持的正规ID列表的一例的图。该图所例示的正规ID列表表示包含ID(消息ID)的值是“1”、“2”、“3”及“4”的某个的消息ID的帧能够流到总线500b中。

[0163] [1.17非法检测计数器保存列表例]

[0164] 图17是表示每个消息ID的非法检测计数器的状态的一例的图。该图的例子表示只有消息ID是“4”的非法检测计数器检测到一次非法,在其他的消息ID中一次也没有检测到。即,该例表示非法检测ECU100a检测到总线500a中本来不应流过的消息ID“4”的消息(帧)被发送了一次、将与相应的消息ID“4”对应的非法检测计数器递增1的情况。

[0165] [1.18有关非法帧的检测的次序]

[0166] 以下,关于在具备上述结构的车载网络系统10的总线500a上连接着非法的ECU的情况,对连接于总线500a的非法检测ECU100a、ECU400a、ECU400b、网关300等的动作进行说明。

[0167] 图18是表示非法检测ECU100a检测到非法的帧(消息)、阻止由其他的ECU进行与该非法的帧对应的处理的动作例的次序图。在该图中,表示非法的ECU向总线500a发送消息ID为“4”、数据字段(数据)为“255(0xFF)”的数据帧的情况的例子。这里的各次序是指各种装置中的各处理顺序(步骤)。

[0168] 首先,非法的ECU开始消息ID为“4”、数据为“255(0xFF)”的数据帧的发送(次序S1001)。将构成帧的各位的值按照上述数据帧格式,以SOF、ID字段(消息ID)的顺序依次向总线500a上送出。

[0169] 当非法的ECU将直到ID字段(消息ID)都向总线500a送出完时,非法检测ECU100a、ECU400a、ECU400b及网关300分别接收消息ID(次序S1002)。

[0170] ECU400a、ECU400b及网关300分别使用所保持的接收ID列表检查消息ID(次序S1003)。此时,非法检测ECU100a使用所保持的正规ID列表检查消息ID(次序S1004)。即,非法检测ECU100a判定被发送的帧中的ID字段的内容是否与表示非法的规定条件(没有登载在正规ID列表中)相符。

[0171] 在次序S1003中,ECU400a及ECU400b由于在分别保持的接收ID列表中不包含“4”(参照图9),所以结束接收。即,这以后不进行非法的ECU继续发送的帧的解释,不进行与帧对应的处理。此外,在次序S1003中,网关300由于在保持的接收ID列表中不包含“4”(参照图5),所以继续接收。此外,在次序S1004中,非法检测ECU100a由于在所保持的正规ID列表中不包含“4”,所以判断是非法的消息ID,接着开始错误帧的发行准备(次序S1005)。

[0172] 接着次序S1003,网关300继续帧的接收。例如,在非法检测ECU100a进行错误帧的发行准备的期间中,从非法的ECU向总线500a上依次送出作为比ID字段靠后的部分的RTR、控制字段(IDE、r、DLC),接着将数据字段每次1位地依次送出。网关300接收该RTR、控制字段(IDE、r、DLC),接着开始数据字段的接收(次序S1006)。

[0173] 接着,错误帧的发行准备结束,非法检测ECU100a发送错误帧(次序S1007)。该错误帧的发送在非法的帧的最末尾被发送之前(例如CRC序列的最末尾被发送之前等)进行。在该动作例中,在数据字段的中途进行。通过开始该错误帧的发送,在总线500a中,从非法的ECU发送中的帧的数据字段的中途部分被错误帧(优先的显性的位序列)覆盖。

[0174] 接收到在次序S1007中发送的错误帧的网关300在数据字段的接收中途将非法的ECU发送的帧的接收中止(次序S1008)。即,网关300由于来自非法的ECU的数据字段被错误帧覆盖而检测到错误帧,所以不继续接收非法的ECU发送的帧。

[0175] 非法检测ECU100a将与作为发送错误帧的对象的数据帧的消息ID“4”对应的非法检测计数器递增(次序S1009)。

[0176] 在作为递增的结果而与消息ID“4”对应的非法检测计数器为17以上的情况下,非法检测ECU100a发送通知错误显示的帧(错误显示消息)以使头单元200接收(次序S1010)。结果,由头单元200的帧处理部220进行用于错误显示的处理,经由LCD等报告错误。另外,错误的报告除了向LCD等的显示以外,也可以通过声音输出、发光等进行。

[0177] [1.19实施方式1的效果]

[0178] 在实施方式1中表示的非法检测ECU关于发送来的帧(数据帧)是否是非法的帧,使用正规ID列表对帧的ID字段进行判定。由此,能够通过数据帧中的ID字段判定非法,所以能够阻止在已有的节点(即非法检测ECU及非法的ECU以外的ECU)中将非法的帧解释而执行与该帧对应的处理。此外,由于仅通过接收与数据帧的开头的SOF接着的ID字段就能够判定,所以与接收数据帧的后部等进行判定的情况相比,能够抑制总线的通信量。

[0179] 此外,非法检测ECU使用非法检测计数器将发送了错误帧的次数进行计数,从而能够检测到通过错误帧的接收而发送非法的消息ID的节点的发送错误计数器达到了若按照CAN协议则应转移为被动状态的上限值的情况。由此,能够判定发送非法的消息ID的节点是否依据CAN协议的错误计数器的规格。

[0180] 此外,通过使进行非法的帧的判定的节点仅为非法检测ECU,能够将对已有的网络结构的影响抑制在最小限度,作为系统整体能够抑制处理量、电力消耗量。

[0181] 另外,也可以是上述车载网络系统10的1或多个非法检测ECU能够切换是否进行检测。并且,也可以仅限于车辆的状态是例如从使用开始起经过了一定期间等的一定的情况,非法检测ECU不进行非法的消息的检测。由此,能够抑制电力消耗量,能够抑制作为车载网络系统10的电力供给源的车载电池的消耗。

[0182] (实施方式2)

[0183] 以下,作为本发明的实施方式,对包括非法检测ECU的车载网络系统11进行说明,该非法检测ECU基于按每个消息ID而容许的数据范围,实现用来阻止在其他节点(ECU)中执行基于非法的帧的处理的非法应对方法。

[0184] [2.1车载网络系统11的整体结构]

[0185] 图19是表示有关实施方式2的车载网络系统11的整体结构的图。车载网络系统11是将在实施方式1中表示的车载网络系统10的一部分变形而得到的。车载网络系统11构成为包括总线500a、500b、和非法检测ECU2100a、2100b、头单元200、网关300及连接于各种设备的ECU400a~400d等ECU这样的连接于总线的各节点。关于车载网络系统11的构成要素中的具有与实施方式1同样的功能的构成要素,赋予相同的标号而省略说明。

[0186] 非法检测ECU2100a、2100b分别连接于总线500a、总线500b,是具有判定由ECU400a~400d等发送的帧是否是非法的、如果是非法则发送错误帧的功能的ECU。

[0187] [2.2非法检测ECU2100a的结构]

[0188] 图20是非法检测ECU2100a的结构图。非法检测ECU2100a构成为包括帧收发部160、

帧解释部2150、非法帧检测部2130、数据范围列表保持部2120、非法检测计数器保持部110和帧生成部140。这些各构成要素是功能性的构成要素,其各功能由非法检测ECU2100a中的通信电路、执行保存在存储器中的控制程序的处理器或数字电路等实现。非法检测ECU2100a是将在实施方式1中表示的非法检测ECU100a的一部分变形而得到的,关于具有与实施方式1同样的功能的构成要素,赋予相同的标号而省略说明。另外,非法检测ECU2100b也具备与非法检测ECU2100a同样的结构。

[0189] 帧解释部2150是将在实施方式1中表示的帧解释部150变形而得到的,从帧收发部160接受帧的值,进行解释以映射到由CAN协议规定的帧格式的各字段。在判断为帧是数据帧的情况下,将判断为数据字段的值(数据)与ID字段的ID(消息ID)一起向非法帧检测部2130转送。此外,帧解释部2150在判断为不符合CAN协议的帧的情况下,向帧生成部140通知以发送错误帧。此外,帧解释部2150在接收到错误帧的情况下,即在根据接受到的帧中的值解释为错误帧的情况下,在其以后将该帧丢弃,即中止帧的解释。

[0190] 非法帧检测部2130是将在实施方式1中表示的非法帧检测部130变形而得到的,接受由帧解释部2150通知的消息ID和数据字段的值(数据),判定这些值是否与表示非法的规定条件相符。即,非法帧检测部2130作为判定接收到的帧中的规定字段的内容是否与表示非法的规定条件相符的所谓判定部发挥功能。该表示非法的规定条件,是数据没有进入在数据范围列表保持部2120保持的数据范围列表中与信息ID建立对应地记载的数据范围中的条件。非法帧检测部2130按照保持在数据范围列表保持部2120中的决定了各消息ID的数据范围的列表即数据范围列表,进行是否是非法的判定。非法帧检测部2130在接收到由数据范围列表表示的范围以外的数据的情况下,为了将非法的检测次数递增,将接收到的消息ID向非法检测计数器保持部110通知。关于在该非法的检测次数达到了一定次数以上的情况下用来发送错误显示消息以由头单元200接收的控制,如在实施方式1中说明的那样,所以省略这里的说明。此外,在接收到由数据范围列表表示的范围以外的数据的情况下,向帧生成部140通知以使其发送错误帧。

[0191] 数据范围列表保持部2120保持数据范围列表,该数据范围列表是关于在车载网络系统11中在总线上被发送的数据帧中包含的数据(数据字段的值)预先规定了容许的范围的列表(参照图21)。

[0192] [2.3数据范围列表例]

[0193] 图21是表示在非法检测ECU2100a的数据范围列表保持部2120中保持的数据范围列表的一例的图。该数据范围列表是将各ID(消息ID)、作为该消息ID的数据帧中的数据字段的值(数据)而被容许的数据范围建立了对应的列表。在图21的例子中,关于消息ID是“1”的数据帧,设为数据范围“0~180”为正常,关于消息ID是“2”或“4”的数据帧,设为数据范围“0~100”为正常,关于消息ID是“3”的数据帧,设为数据范围“0、1”为正常。

[0194] [2.4有关非法帧的检测的次序]

[0195] 以下,关于非法的ECU连接到具备上述结构的车载网络系统11的总线500a的情况,说明连接于总线500a的非法检测ECU2100a、ECU400a、ECU400b,网关300等的动作。

[0196] 图22及图23是表示非法检测ECU2100a检测到非法的帧(消息)、阻止由其他ECU进行与该非法的帧对应的处理的动作例的次序图。在图22及图23中,与在实施方式1中表示的图18的情况同样,表示非法的ECU向总线500a发送消息ID为“4”、数据字段(数据)为“255

(0xFF)”的数据帧的情况的例子。对于与在实施方式1中表示的次序相同的次序赋予相同的标号,这里将说明简略化。

[0197] 首先,非法的ECU开始非法的数据帧的发送(次序S1001)。非法检测ECU2100a、ECU400a、ECU400b及网关300分别接收消息ID(次序S1002)。ECU400a、ECU400b及网关300分别使用所保持的接收ID列表检查消息ID(次序S1003)。ECU400a及ECU400b由于在分别所保持的接收ID列表中不包含“4”(参照图9),所以结束接收。网关300由于在所保持的接收ID列表中不包含“4”(参照图5),所以继续接收,进行数据字段的接收(次序S1006a)。同样,非法检测ECU2100a也进行数据字段的接收(次序S1006a)。

[0198] 接着次序S1006a,非法检测ECU2100a使用数据范围列表(参照图21)检查数据字段的数据(次序S2001)。即,非法检测ECU2100a判定发送来的帧中的ID字段的内容是否与表示非法的规定条件(没有进入到数据范围列表中所记载的数据的范围中)相符。非法检测ECU2100a由于在数据范围列表中没有记载与ID“4”对应的“255(0xFF)”的值,所以判断为是非法的数据帧,接着开始错误帧的发行准备(次序S1005)。

[0199] 在非法检测ECU2100a进行错误帧的发行准备的期间中,从非法的ECU将作为比数据字段靠后的部分的CRC字段(CRC序列及CRC定界符)每次1位地依次送出至总线500a上。网关300开始该CRC字段的接收(次序S2002)。

[0200] 接着,错误帧的发行准备结束,非法检测ECU2100a发送错误帧(次序S1007)。通过开始该错误帧的发送,在总线500a中,从非法的ECU发送中的帧的CRC序列的中途部分被错误帧(优先的显性的位序列)覆盖。

[0201] 接收到在次序S1007中发送的错误帧的网关300在包含CRC序列的CRC字段的接收中途,将非法的ECU发送的数据帧的接收中止(次序S2003)。即,网关300由于来自非法的ECU的CRC序列被错误帧覆盖、检测到错误帧,所以不继续接收非法的ECU发送的数据帧。

[0202] 非法检测ECU2100a将与作为发送错误帧的对象的数据帧的ID“4”对应的非法检测计数器递增(次序S1009)。在作为递增的结果而与ID“4”对应的非法检测计数器为17以上的情况下,非法检测ECU2100a发送错误显示消息(次序S1010)。

[0203] [2.5实施方式2的效果]

[0204] 在实施方式2中表示的非法检测ECU关于发送来的帧是否是非法的帧,使用数据范围列表对帧(数据帧)的ID字段及数据字段进行判定。由此,能够通过数据帧中的ID字段与数据字段的组合来判定非法,所以能够阻止在已有的ECU(即非法检测ECU及非法的ECU以外的ECU)中将非法的帧解释而执行与该帧对应的处理。此外,由于仅通过接收到数据帧的数据字段就能够判定,所以与接收数据帧的后部而进行判定的情况相比能够抑制总线的通信量。

[0205] 此外,非法检测ECU使用非法检测计数器将发送了错误帧的次数进行计数,从而能够检测到通过错误帧的接收而发送非法的消息ID的节点的发送错误计数器达到了若按照CAN协议则应转移为被动状态的上限值的情况。由此,能够判定发送非法的消息ID的节点是否依据CAN协议的错误计数器的规格。

[0206] 此外,通过使进行非法的帧的判定的节点仅为非法检测ECU,能够将对已有的网络结构的影响抑制在最小限度,作为系统整体能够抑制处理量、电力消耗量。

[0207] 另外,也可以是上述车载网络系统11的1个或多个非法检测ECU能够切换是否进行

检测。并且,也可以仅限于车辆的状态是例如从使用开始起经过了一定期间等的一定的情况,非法检测ECU不进行非法的消息的检测。由此,能够抑制电力消耗量。

[0208] (实施方式3)

[0209] 以下,作为本发明的实施方式,对包括非法检测ECU的车载网络系统12进行说明,该非法检测ECU使用根据消息ID、数据及计数器值计算的消息认证代码(MAC:Message Authentication Code),实现于用来阻止在其他节点(ECU)中执行基于非法的帧的处理的非法应对方法。

[0210] [3.1车载网络系统12的整体结构]

[0211] 图24是表示有关实施方式3的车载网络系统12的整体结构的图。车载网络系统12是将在实施方式1中表示的车载网络系统10的一部分变形而得到的。车载网络系统12构成为包括总线500a、500b、和非法检测ECU3100a、3100b、头单元200、网关300及连接于各种设备的ECU3400a~3400d等ECU这样的连接于总线的各节点。对于车载网络系统12的构成要素中的具有与实施方式1同样的功能的构成要素,赋予相同的标号而省略说明。

[0212] 非法检测ECU3100a、3100b分别连接于总线500a、总线500b,是具有判定由ECU3400a~3400d等发送的帧是否是非法的、如果是非法则发送错误帧的功能的ECU。

[0213] ECU3400a~3400d与某个总线连接,此外,分别连接于发动机401、制动器402、门开闭传感器403、窗开闭传感器404。ECU3400a~3400d分别取得所连接的设备(发动机401等)的状态,定期地将表示状态的数据帧向网络(即总线)发送。对于被发送的数据帧的数据字段,赋予根据消息ID、数据值和每当发送时递增的计数器值通过计算导出的消息认证代码(MAC)。

[0214] [3.2ECU3400a的结构]

[0215] 图25是ECU3400a的结构图。ECU3400a构成为包括帧收发部460、帧解释部450、接收ID判断部430、接收ID列表保持部440、帧处理部410、帧生成部3420、数据取得部470、MAC生成部3410、MAC密钥保持部3430和计数器保持部3440。这些各构成要素是功能性的构成要素,其各功能由ECU3400a中的通信电路、执行保存在存储器中的控制程序的处理器或数字电路等实现。ECU3400a是将在实施方式1中表示的ECU400a的一部分变形而得到的,对于具有与实施方式1同样的功能的构成要素赋予相同的标号而省略说明。

[0216] 帧生成部3420是将在实施方式1中表示的帧生成部420的一部分变形而得到的。帧生成部3420按照从帧解释部450通知的指示错误帧的发送的通知,构成错误帧,将错误帧向帧收发部460通知而使其发送。此外,帧生成部3420将由数据取得部470通知的数据的值和预先决定的消息ID向MAC生成部3410通知,接受计算出的MAC。帧生成部3420以包含预先决定的消息ID、由数据取得部470通知的数据的值和从MAC生成部3410接受到的MAC的方式构成帧(参照图26),向帧收发部460通知。

[0217] MAC生成部3410对于将由帧生成部3420通知的消息ID、数据的值和由计数器保持部3440保持的计数器值结合而得到的值(结合值),使用由MAC密钥保持部3430保持的MAC密钥,计算(通过计算导出)MAC,将作为该计算出的结果的MAC向帧生成部3420通知。这里,作为MAC的计算方法,采用HMAC(Hash-based Message Authentication Code)(参照非专利文献2),对上述结合值,以填充到规定的块量(例如4bytes)的值使用MAC密钥进行计算,将得出的计算结果的开头4bytes作为MAC。另外,这里,为了计算MAC而使用的结合值,使用消

息ID、数据的值和由计数器保持部3440保持的计数器值,但也可以使用它们3个中的某1个或两个的组合来计算MAC。

[0218] MAC密钥保持部3430保持为了计算MAC所需要的MAC密钥。

[0219] 计数器保持部3440保持为了计算MAC所需要的计数器值。另外,该计数器值每当在帧收发部460中正常地发送了数据帧时递增。

[0220] 另外,ECU3400b~3400d是分别将在实施方式1中表示的ECU400b~400d的一部分变形而得到的,具备与上述ECU3400a基本上同样的结构。但是,在接收ID列表保持部440中保持的接收ID列表的内容可以按每个ECU而不同。例如ECU3400a及ECU3400b保持图9所例示的接收ID列表,ECU3400c及ECU3400d保持图5所例示的接收ID列表。此外,帧处理部410的处理内容如在实施方式1中表示那样按每个ECU而不同。以下,使用图26~图29说明ECU3400a~3400d分别发送的帧的内容。

[0221] [3.3有关发动机的ECU3400a的发送帧例]

[0222] 图26是表示从连接于发动机401的ECU3400a发送的数据帧的ID(消息ID)及数据字段(数据)的一例的图。ECU3400a发送的帧的消息ID是“1”。关于数据,在该图中按每1字节用空白划分而表示,开头的1byte表示时速(km/时),接着的1byte表示计数器值,接着的4bytes表示MAC。另外,在图26的例子中MAC用16进制数表述。开头1byte的时速(km/时)取最低0(km/时)~最高180(km/时)的范围的值。从图26的上行向下行,例示与从ECU3400a依次发送的各帧对应的各消息ID及数据,表示计数器值逐渐增加、时速从0km/时起每次加速1km/时的情形。

[0223] [3.4有关制动器的ECU3400b的发送帧例]

[0224] 图27是表示从与制动器402连接的ECU3400b发送的数据帧的ID(消息ID)及数据字段(数据)的一例的图。ECU3400b发送的帧的消息ID是“2”。关于数据,在该图中按每1字节用空白划分而表示,开头的1byte用比例(%)表示制动的施加状况,接着的1byte表示计数器值,接着的4bytes表示MAC。另外,在图27的例子中,用16进制数表示MAC。开头1byte的制动的施加状况中,设完全没有施加制动的状态为0(%)、设最大限度施加制动的状态为100(%)。从图27的上行向下行,例示了与从ECU3400b依次发送的各帧对应的各消息ID及数据,表示计数器值逐渐增加、关于制动从100%起逐渐将制动器减弱的情形。

[0225] [3.5有关门开闭传感器的ECU3400c的发送帧例]

[0226] 图28是表示从与门开闭传感器403连接的ECU3400c发送的数据帧的ID(消息ID)及数据字段(数据)的一例的图。ECU3400c发送的帧的消息ID是“3”。关于数据,在该图中按每1字节用空白划分而表示,开头的1byte表示门的开闭状态,接着的1byte表示计数器值,接着的4bytes表示MAC。另外,在图28的例子中,用16进制数表示MAC。开头1byte的门的开闭状态中,设门打开的状态为“1”、设门关闭的状态为“0”。从图28的上行向下行,例示与从ECU3400c依次发送的各帧对应的各消息ID及数据,表示计数器值逐渐增加、门从打开的状态起逐渐向关闭的状态转移的情形。

[0227] [3.6有关窗开闭传感器的ECU3400d的发送帧例]

[0228] 图29是表示从与窗开闭传感器404连接的ECU3400d发送的数据帧的ID(消息ID)及数据字段(数据)的一例的图。ECU3400d发送的帧的消息ID是“4”。关于数据,在该图中按每1字节用空白划分而表示,开头的1byte用比例(%)表示窗的开闭状态,接着的1byte表示计

数器值,接着的4bytes表示MAC。另外,在图29的例子中,用16进制数表示MAC。开头1byte的窗的开闭状态中,设窗完全关闭的状态为0(%)、设窗全开的状态为100(%)。从图29的上行向下行,例示与从ECU3400d依次发送的各帧对应的各消息ID及数据,表示计数器值逐渐增加、窗从关闭的状态逐渐打开的情形。

[0229] [3.7非法检测ECU3100a的结构]

[0230] 图30是非法检测ECU3100a的结构图。非法检测ECU3100a由帧收发部160、帧解释部3150、非法MAC检测部3130、MAC密钥保持部3180、计数器保持部3190、帧生成部140、MAC生成部3170和非法检测计数器保持部110构成。这些各构成要素是功能性的构成要素,该各功能由非法检测ECU3100a中的通信电路、执行保存在存储器中的控制程序的处理器或数字电路等实现。非法检测ECU3100a是将在实施方式1中表示的非法检测ECU100a的一部分变形而得到的,对具有与实施方式1同样的功能的构成要素赋予相同的标号而省略说明。另外,非法检测ECU3100b也是同样的结构。

[0231] 帧解释部3150是将在实施方式1中表示的帧解释部150变形而得到的,从帧收发部160接受帧的值,进行解释以映射到由CAN协议规定的帧格式的各字段。在判断为帧是数据帧的情况下,将判断为数据字段的值(数据)与ID字段的ID(消息ID)一起向非法MAC检测部3130转送。此外,帧解释部3150在判断为不符合CAN协议的帧的情况下,向帧生成部140通知以发送错误帧。此外,帧解释部3150在接收到错误帧的情况下,即在根据接受到的帧中的值解释为错误帧的情况下,在其以后将该帧丢弃,即中止帧的解释。

[0232] 非法MAC检测部3130具有接受由帧解释部3150通知的消息ID和数据字段的值(数据)并对数据字段中的MAC进行验证的功能。非法MAC检测部3130将被通知的消息ID及数据字段的值向MAC生成部3170通知,取得由MAC生成部3170生成的MAC。非法MAC检测部3130判定数据字段的数据是否与表示非法的规定条件相符。即,非法MAC检测部3130作为判定接收到的帧中的规定字段的内容是否与表示非法的规定条件相符的所谓判定部发挥功能。该表示非法的规定条件是规定的验证处理顺序(包括MAC的生成、MAC的比较等的顺序)中的验证失败,即,数据中包含的MAC与由MAC生成部3170生成的MAC不同的条件。非法MAC检测部3130通过将从MAC生成部3170取得的MAC与数据字段中的MAC比较,进行是否非法的判定(即MAC的验证)。在两MAC的值的比较的结果为不一致的情况下,为了将非法的检测次数递增,将接收到的消息ID向非法检测计数器保持部110通知。在该非法的检测次数达到一定次数以上的情况下,用来发送错误显示消息以便由头单元200接收的控制如在实施方式1中说明那样,所以省略这里的说明。此外,在两MAC的值的比较的结果不一致的情况下,向帧生成部140通知以发送错误帧。在MAC值的比较的结果一致的情况下,向MAC生成部3170通知以将计数器保持部3190保持的与消息ID对应的计数器值递增。

[0233] MAC生成部3170使用由非法MAC检测部3130通知的消息ID,从MAC密钥保持部3180取得对应的MAC密钥,从计数器保持部3190分别取得对应的计数器。MAC生成部3170对由非法MAC检测部3130通知的数据字段的值(开头1byte的值)和从计数器保持部3190取得的计数器值,使用从MAC密钥保持部3180取得的MAC密钥计算(通过计算导出)MAC,将计算出的MAC向非法MAC检测部3130通知。另外,在非法检测ECU3100a、3100b及ECU3400a~3400d中,使用MAC密钥计算MAC的算法都使用相同的算法。

[0234] MAC密钥保持部3180将为了计算MAC所需要的MAC密钥按每个消息ID建立对应而保

持。该MAC密钥保持部3180保持的MAC密钥是按建立了对应的每个消息ID而不同的值。另外,关于在ECU及非法检测ECU中使用的MAC密钥,如果设想1个发送节点发送多个消息ID各自的帧的情况,则也可以是按每个发送节点而不同的密钥。此外,MAC密钥例如也可以在相同的总线上被发送的帧中使用相同的值,也可以即使在不同的总线上也使用相同的密钥(值),也可以每一台车使用相同的密钥,也可以相同车种使用相同的密钥,也可以相同的制造厂商使用相同的密钥,也可以即使是不同的制造厂商也使用相同的密钥。

[0235] 计数器保持部3190将为了计算MAC值所需要的计数器值按每个消息ID保持。该计数器值在正常地接收到帧的情况下(即在非法MAC检测部3130中比较的两MAC一致的情况下)递增。

[0236] [3.8计数器值的例子]

[0237] 图31是表示保持在计数器保持部3190中的各消息ID的计数器值的一例的图。在该图中,消息ID为“1”的计数器表示1次,消息ID为“2”的计数器表示10次,消息ID为“3”的计数器表示15次,消息ID为“4”的计数器表示100次。与该各消息ID对应的计数器值表示包含该消息ID的帧被正常地接收的次数。

[0238] [3.9有关非法帧的检测的次序]

[0239] 以下,关于在具备上述结构的车载网络系统12的总线500a上连接着非法的ECU的情况,对连接于总线500a的非法检测ECU3100a、ECU3400a、ECU3400b、网关300等的动作进行说明。

[0240] 图32及图33是表示非法检测ECU3100a检测到非法的帧(消息)、阻止由其他的ECU进行与该非法的帧对应的处理的动作例的次序图。在图32及图33中,与在实施方式1中表示的图18及在实施方式2中表示的图22及图23的情况同样,表示非法的ECU连接于总线500a的例子。该非法的ECU发送消息ID为“4”、数据字段(数据)为“0xFF FF FFFFFFFF”(6bytes)的数据帧。对于与在实施方式1或2中表示的次序相同的次序赋予相同的标号,这里将说明简化。

[0241] 首先,非法的ECU开始上述非法的数据帧的发送(次序S1001a)。非法检测ECU3100a、ECU3400a、ECU3400b及网关300分别接收消息ID(次序S1002)。ECU3400a、ECU3400b及网关300分别使用所保持的接收ID列表检查消息ID(次序S1003)。ECU3400a及ECU3400b由于在分别保持的接收ID列表中不包含“4”(参照图9),所以结束接收。网关300由于在保持的接收ID列表中包含“4”(参照图5),所以继续接收而进行数据字段的接收(次序S1006a)。同样,非法检测ECU3100a也进行数据字段的接收(次序S1006a)。

[0242] 接着次序S1006a,非法检测ECU3100a验证(检查)数据字段的数据中包含的MAC(次序S3001)。即,非法检测ECU3100a判定被发送的帧的ID字段的内容是否与表示非法的规定条件(MAC的验证失败)相符。非法检测ECU3100a关于由非法的ECU发送来的数据帧中的数据字段的6bytes的数据“0xFFFFFFFF”,将后半4bytes的MAC与使用与消息ID“4”对应的MAC密钥和计数器计算出的MAC进行比较,进行MAC的验证。由于该比较的结果为不一致,验证失败,所以在非法检测ECU3100a中,判断为是非法的数据帧,接着开始错误帧的发行准备(次序S1005)。

[0243] 在非法检测ECU3100a进行错误帧的发行准备的期间中,网关300开始CRC字段的接收(次序S2002)。

[0244] 接着,错误帧的发行准备结束,非法检测ECU3100a发送错误帧(次序S1007)。通过开始该错误帧的发送,在总线500a中,从非法的ECU发送中的帧的CRC序列的中途部分被错误帧覆盖。

[0245] 接收到在次序S1007中发送的错误帧的网关300在包括CRC序列的CRC字段的接收中途,将非法的ECU发送的数据帧的接收中止(次序S2003)。

[0246] 非法检测ECU3100a将与作为发送错误帧的对象的数据帧的ID“4”对应的非法检测计数器递增(次序S1009)。在作为递增的结果而与ID“4”对应的非法检测计数器成为17以上的情况下,非法检测ECU3100a发送错误显示消息(次序S1010)。

[0247] [3.10实施方式3的效果]

[0248] 在实施方式3中表示的非法检测ECU关于发送来的帧是否是非法的帧,通过验证帧(数据帧)的数据字段中包含的MAC来判定。由此,能够阻止在已有的ECU(即非法检测ECU及非法的ECU以外的ECU)中将非法的帧解释而执行与该帧对应的处理。此外,由于仅通过接收到数据帧的数据字段就能够判定,所以与接收数据帧的后部而进行判定的情况相比能够抑制总线的通信量。

[0249] 此外,非法检测ECU使用非法检测计数器将发送了错误帧的次数进行计数,由此能够检测到通过错误帧的接收而发送非法的消息ID的节点的发送错误计数器达到了若按照CAN协议则应转移为被动状态的上限值的情况。由此,能够判定发送非法的消息ID的节点是否依据CAN协议的错误计数器的规格。

[0250] 此外,通过使进行MAC的验证的节点仅为非法检测ECU,不需要由非法检测ECU以外的ECU进行验证,作为系统整体能够抑制处理量、电力消耗量。

[0251] 另外,也可以是上述车载网络系统12中的1个或多个非法检测ECU能够切换是否进行检测。并且,也可以仅限于车辆的状态为例如从使用开始起经过了一定期间等的一定的情况,非法检测ECU不进行非法的消息的检测。由此,能够抑制电力消耗量。

[0252] (实施方式4)

[0253] 以下,作为本发明的实施方式,对实现非法检测方法的车载网络系统13进行说明,该非法检测方法用来根据车辆的状态来切换与是否执行检测非法的消息(帧)的特定的检测处理有关的非法检测ECU的动作模式。

[0254] [4.1车载网络系统13的整体结构]

[0255] 图34是表示有关实施方式4的车载网络系统13的整体结构的图。车载网络系统13是将在实施方式1中表示的车载网络系统10的一部分变形而得到的。车载网络系统13构成包括总线500a~500c、和非法检测ECU4100a、4100b、头单元4200、网关300及连接于各种设备的ECU400a~400d等的ECU这样的连接于总线的各节点。对于车载网络系统13的构成要素中的具有与实施方式1同样的功能的构成要素赋予相同的标号而省略说明。

[0256] 非法检测ECU4100a、4100b分别连接于总线500a、总线500b,是具有判定由ECU400a~400d等发送的帧(消息)是否是非法的、如果是非法则发送错误帧的功能的ECU。非法检测ECU4100a、4100b是分别将在实施方式1中表示的非法检测ECU100a、100b的一部分变形而得到的。非法检测ECU4100a、4100b作为动作模式而具有判定ECU400a~400d发送的帧(消息)是否为非法的检查模式(检测模式)、和不判定ECU400a~d发送的帧(消息)是否为非法的待机模式。并且,非法检测ECU4100a、4100b具有接受来自头单元4200的指示(触发帧)而切换

动作模式的功能。触发帧是作为动作模式的切换的触发的切换指示消息。在使动作模式为待机模式的情况下,将有关非法的消息的检测的一定的处理省略,所以与检查模式的情况相比能够实现处理量的减少、消耗电力的抑制等。

[0257] 头单元4200具有收发帧的功能,具有将从ECU400a~400d发送的帧接收、将各种状态显示在显示器(未图示)上而向用户提示的功能。头单元4200是将在实施方式1中表示的头单元200的一部分变形而得到的。头单元4200具有判定例如ECU400a~400d发送的帧是否为非法的、在发送了非法的帧的情况下向非法检测ECU4100a、4100b指示向检查模式的切换的功能。即,头单元4200具有在车辆的状态满足一定条件的情况下向非法检测ECU4100a、4100b发送触发帧以指示其变更动作模式的功能。一定条件是用来判断是否发生了影响由非法检测ECU检测非法的消息的必要性的的高低的事件的条件。作为将动作模式向检查模式切换的情况的一定条件,例如在搭载于车辆中的车载网络系统中,可以举出检测到被传送了非法的消息的情况、开始了车辆的使用的情况、成为与车辆的外部的装置开始通信的状态的情况等。此外,作为将动作模式向待机模式切换的情况的一定条件,例如可以举出在一定期间中没有检测到非法的消息的情况、从开始车辆的使用起经过了一定时间的情况、与车辆的外部的装置结束通信而成为一定状态的情况等的各自或多个的组合等。

[0258] 另外,在本实施方式中,假设网关300在总线500a~500c间转送触发帧。

[0259] [4.2头单元4200的结构]

[0260] 图35是头单元4200的结构图。头单元4200构成为包括帧收发部270、帧解释部4260、接收ID判断部240、接收ID列表保持部250、帧处理部220、显示控制部210、帧生成部4230、非法帧检测部4280、模式变更指示部4281、车使用开始检测部4282和通信开始/结束检测部4283。这些各构成要素是功能性的构成要素,其各功能由头单元4200中的通信电路、LCD、执行保存在存储器中的控制程序的处理器或数字电路等实现。另外,对于具有与实施方式1同样的功能的构成要素赋予相同的标号而省略说明。

[0261] 帧解释部4260是将在在实施方式1中表示的帧解释部260的一部分变形而得到的。帧解释部4260从帧收发部270接受帧的值,进行解释以映射到由CAN协议规定的帧格式的各字段。帧解释部4260将判断为ID字段的值向接收ID判断部240转送。帧解释部4260根据由接收ID判断部240通知的判定结果,决定是将ID字段的值和ID字段以后出现的数据字段向帧处理部220及非法帧检测部4280转送、还是在接受到其判定结果以后将帧的接收中止(即,将作为该帧的解释中止)。此外,帧解释部4260在判断为是不符合CAN协议的帧的情况下,向帧生成部4230通知以使其发送错误帧。此外,帧解释部4260在接收到错误帧的情况下,即在根据接受到的帧中的值解释为错误帧的情况下,在其以后将该帧丢弃,即中止帧的解释。例如在从数据帧的中途被解释为错误帧的情况下,将该数据帧的解释中止,不再根据该数据帧进行特别的处理。

[0262] 帧收发部270对总线500c收发遵循CAN协议的帧。从总线500c每次1bit地接收帧,向帧解释部4260转送。此外,将从帧生成部4230接受到通知的帧的内容向总线500c每次1bit地发送。

[0263] 接收ID判断部240接受从帧解释部4260通知的ID字段的值,按照接收ID列表保持部250保持的消息ID的列表,进行是否接收该ID字段以后的帧的各字段的判定。接收ID判断部240将该判定结果向帧解释部4260通知。

[0264] 帧生成部4230与实施方式1的帧生成部230同样,按照来自帧解释部4260的、指示错误帧的发送的通知,构成错误帧,将错误帧向帧收发部270通知而使其发送。进而,帧生成部4230按照来自模式变更指示部4281的触发帧的发送的委托,构成触发帧,将触发帧向帧收发部270通知而使其发送。

[0265] 非法帧检测部4280接受由帧解释部4260通知的ID字段的值和数据字段的值,在非法的帧被发送到总线500c上的情况下检测到。非法帧检测部4280在检测到非法的帧的情况下,向模式变更指示部4281委托非法检测ECU4100a、4100b的向检查模式的转移指示的通知。非法帧检测部4280也可以在从委托向检查模式的转移指示的通知起一定期间中没有检测到非法的帧的情况下,向模式变更指示部4281委托非法检测ECU4100a、4100b的向待机模式的转移指示的通知。非法帧检测部4280的非法帧的检测方法例如是与实施方式1的非法帧检测部130相同的方法。此外,非法帧检测部4280的非法帧的检测方法例如也可以是与实施方式2的非法帧检测部2130相同的方法、与实施方式3的非法MAC检测部3130相同的方法或其他方法。

[0266] 模式变更指示部4281具有向帧生成部4230委托指示非法检测ECU4100a、4100b的动作模式的变更的触发帧向非法检测ECU4100a、4100b的发送的功能。模式变更指示部4281在车辆的状态满足一定条件的情况下,从非法帧检测部4280、车使用开始检测部4282或通信开始/结束检测部4283接受委托,向帧生成部4230进行触发帧的发送的委托。该触发帧是作为非法检测ECU的动作模式的切换的触发的切换指示消息。在触发帧中,有指示从待机模式向检查模式的转移的帧、指示从检查模式向待机模式的转移的帧,两者例如用ID字段的消息ID、设在数据字段内的识别码等区别。如果发送了触发帧,则网关300在总线间转送触发帧,各非法检测ECU接收触发帧。

[0267] 车使用开始检测部4282检测开始了车辆的使用的情况,向模式变更指示部4281委托非法检测ECU4100a、4100b的向检查模式的转移指示的通知。车使用开始检测部4282例如通过根据来自各ECU的消息等对门锁止的解除、门的打开、发动机的启动等,来实现开始了车辆的使用的情况的检测。结果,例如在停车在停车场中的车辆上安装着非法ECU的情况下,在其后开始使用车辆时,非法检测ECU4100a、4100b成为检查模式而也能够进行非法ECU的检测。另外,在车辆的使用开始前,如果从电池等供给电力,车载网络系统也能够工作。此外,车使用开始检测部4282检测从检测到开始了车辆的使用起经过了一定时间的情况,向模式变更指示部4281委托非法检测ECU4100a、4100b的向待机模式的转移指示的通知。该一定时间是比设想在车辆的使用开始前假设非法的ECU连接到车载网络系统的总线上的情况下、在车辆的使用开始后该非法的ECU发送非法的消息所需要的时间长的时间(例如几分钟)。

[0268] 通信开始/结束检测部4283检测头单元4200开始与外部通信的情况,向模式变更指示部4281委托非法检测ECU4100a、4100b的向检查模式的转移指示的通知。结果,例如在从外部通过通信经由头单元4200非法地将非法的帧发送到车载网络系统的总线上的情况下,能够由检查模式的非法检测ECU4100a、4100b进行非法的检测。另外,可以想到通过从外部的通信,头单元4200的控制程序被非法地改写,非法帧检测部4280、模式变更指示部4281等不再发挥功能。但是,通过在与外部的通信之前向非法检测ECU4100a、4100b指示向检查模式的转移,即使非法帧检测部4280、模式变更指示部4281等不再发挥功能,也能够检测非

法的帧。此外,通信开始/结束检测部4283检测头单元4200成为结束与外部的通信后的一定状态的情况,向模式变更指示部4281委托非法检测ECU4100a、4100b的向待机模式的转移指示的通知。结束与外部的通信后的一定状态,例如是结束了与外部的通信的状态。此外,结束与外部的通信后的一定状态也可以是在结束与外部的通信后经过了一定时间的状态。由此,能够应对通过与外部的通信被非法地改写的控制程序在与外部的通信的结束后发送非法的帧的情况。该情况下的一定时间,是比设想在通过与外部的通信从外部供给了非法的程序等的情况下、在通信结束后执行该程序而发送非法的消息所需要的时间长的时间(例如几分钟)。

[0269] 另外,模式变更指示部4281也可以与非法帧检测部4280、车使用开始检测部4282及通信开始/结束检测部4283协同,仅限于在一定期间中没有检测到非法的消息、并且从开始车辆的使用起经过了一定时间、并且与车辆的外部的装置结束通信而成为一定状态的情况,向帧生成部4230委托指示向待机模式的转移的触发帧的发送。模式变更指示部4281关于根据车辆的状态、在满足怎样的条件时委托触发帧的发送,可以保持作为判断基准的预先决定的规则。该规则既可以是单一的,也可以是多个。此外,规则可以在头单元4200出厂时、搭载车载网络系统的车辆出厂时、销售时等设定。此外,也可以是头单元4200从外部通过通信取得及更新规则。此外,也可以将头单元4200构成为,使得保持规则的记录介质拆装自如。另外,也可以设定以作为车辆的状态而检测停车中、刹车中、加油中、充电中、与外部通信中等为前提的规则。也可以通过使触发帧的内容(例如数据字段内)包含例如单独识别非法检测ECU的信息等,仅向特定的非法检测ECU指示动作模式的变更。例如,也可以设定以下规则:在停车中在与外部通信中检测到非法的帧、从非法帧检测部4280委托了非法检测ECU4100a、4100b的向检查模式的转移指示的通知的情况下,判断为仅向非法检测ECU4100b发送指示向检查模式的转移的触发帧。这是认为如果是停车中则不发送对发动机401或制动器402的动作带来影响的非法的帧、或者即使发送了非法的帧、只要是停车中就没有问题的情况的规则的例子。另外,在以对特定的非法检测ECU指示动作模式的变更的方式构成触发帧的情况下,网关300也可以仅向为了向该特定的非法检测ECU传递触发帧所需要的总线进行触发帧的转送。

[0270] [4.3非法检测ECU4100a的结构]

[0271] 图36是非法检测ECU4100a的结构图。非法检测ECU4100a构成为包括帧收发部160、帧解释部4150、非法帧检测部130、正规ID列表保持部120、非法检测计数器保持部110、帧生成部140、触发帧检测部4170和模式保持部4180。这些各构成要素是功能性的构成要素,其各功能由非法检测ECU4100a中的通信电路、执行保存在存储器中的控制程序的处理器或数字电路等实现。对具有与实施方式1同样的功能的构成要素赋予相同的标号而省略说明。另外,非法检测ECU4100b也基本上具备同样的结构。

[0272] 帧解释部4150与实施方式1的帧解释部150同样,从帧收发部160接受帧的值,进行解释以映射到由CAN协议规定的帧格式的各字段。此外,帧解释部4150从模式保持部4180取得非法检测ECU4100a的动作模式,根据动作模式判断接受到的帧的值的转送目的地。例如,在非法检测ECU4100a是检查模式的情况下,将ID字段的值向非法帧检测部130和触发帧检测部4170转送,将ID字段之后的数据字段的值向触发帧检测部4170转送。在非法检测ECU4100a是待机模式的情况下,将ID字段的值和其后的数据字段的值仅向触发帧检测部

4170转送。由此,仅限于动作模式是检查模式的情况,进行由非法帧检测部130实施的非法的检测。即,在动作模式是待机模式的情况下,不进行由非法帧检测部130实施的有关非法的检测的处理。

[0273] 触发帧检测部4170判断非法检测ECU4100a接收到的帧是否是头单元4200发送的触发帧。触发帧检测部4170在非法检测ECU4100a接收到的帧是触发帧的情况下,在模式保持部4180中记录作为动作模式的检查模式或待机模式。即,触发帧检测部4170在接收到的帧是指示从待机模式向检查模式的转移的触发帧的情况下,记录是检查模式。此外,触发帧检测部4170在接收到的帧是指示从检查模式向待机模式的转移的触发帧的情况下,记录是待机模式。

[0274] 模式保持部4180具有将本机(非法检测ECU4100a)的动作模式是待机模式还是检查模式保持到存储器等存储介质中的功能。

[0275] [4.4有关向检查模式的转移的次序]

[0276] 以下,说明向具备上述结构的车载网络系统13的总线500c发送了非法的帧(消息)的情况下的头单元4200及非法检测ECU4100a的动作。

[0277] 图37是表示头单元4200检测非法的消息、向非法检测ECU4100a指示向检查模式的转移、非法检测ECU4100a向检查模式转移的动作例的次序图。

[0278] 在该动作例的开始阶段,非法检测ECU4100a为待机模式(次序S4001)。例如,是作为在该阶段以前非法检测ECU4100a接受到指示向待机模式的转移的触发帧的结果成为待机模式的状态。此时,非法检测ECU4100a不进行由非法帧检测部130实施的非法的消息的检测。

[0279] 头单元4200将发送到总线500c的帧(消息)接收(次序S4002)。

[0280] 头单元4200确认由非法帧检测部4280接收到的消息是否是非法的消息(次序S4003)。在不是非法的消息的情况下,回到消息的接收的处理顺序(次序S4002)。

[0281] 头单元4200在检测到接收到的消息是非法的消息的情况下,根据以前的向非法检测ECU4100a的指示履历,判断非法检测ECU4100a的动作模式是否已经是检查模式(次序S4004)。另外,非法的消息例如可能是非法的ECU连接到总线上而发送。头单元4200在通过触发帧向非法检测ECU4100a等进行了向检查模式的转移指示或向待机模式的转移指示的情况下保持指示履历等,由此掌握各非法检测ECU的动作模式。

[0282] 头单元4200在判断为非法检测ECU4100a的动作模式不是检查模式(是待机模式)的情况下,指示向检查模式的转移(次序S4005)。具体而言,头单元4200发送指示向检查模式的转移的触发帧。另外,在次序S4004中判断为非法检测ECU4100a的动作模式已经是检查模式的情况下,头单元4200将向检查模式的转移的指示的处理顺序跳过而结束动作。

[0283] 从头单元4200发送到总线500c的、指示向检查模式的转移的触发帧由网关300向总线500a、500b转送。

[0284] 非法检测ECU4100a将发送到总线500a的触发帧接收,将动作模式向检查模式转移(次序S4006)。从此时起,非法检测ECU4100a通过非法帧检测部130进行非法的消息的检测。即,在检查模式中,非法检测ECU4100a成为实现用来阻止在其他节点(ECU)中执行基于非法的帧的处理的非法应对方法的状态。因而,如在实施方式1中表示那样,即使向连接着非法检测ECU4100a的总线上发送非法的消息,也能够阻止对应于该非法的消息进行处理(参照

图18)。

[0285] 这里,着眼于非法检测ECU中的非法检测ECU4100a进行了说明,但例如关于非法检测ECU4100b也同样,可以与在次序S400中发送的触发帧对应地将动作模式设为检查模式。此外,头单元4200也可以将次序S4004中的判断省略而进行次序S4005中的向检查模式的转移的指示。在将次序S4004中的判断省略的情况下,可以不掌握各非法检测ECU的动作模式,能够将指示履历的保持省略。但是,次序S4004有利于防止无用的触发帧流到总线中。

[0286] 在这里表示的次序S4003的情况以外,向检查模式的转移例如在通信开始/结束检测部4283检测到与外部的通信开始的情况下、或在车使用开始检测部4282检测到车辆的使用开始的情况下进行。

[0287] [4.5有关向待机模式的转移的次序(与外部的通信结束时)]

[0288] 以下,对头单元4200结束了与外部的通信的情况下的头单元4200及非法检测ECU4100a的动作进行说明。

[0289] 图38是表示头单元4200检测到与外部的通信的结束、向非法检测ECU4100a指示向待机模式的转移、非法检测ECU4100a向待机模式转移的动作例的次序图。

[0290] 在该动作例的开始阶段,非法检测ECU4100a为检查模式(次序S4101)。例如,是作为在该阶段以前非法检测ECU4100a接受到头单元4200在开始与外部的通信时指示向检查模式的转移的触发帧的结果成为检查模式的状态。此时,非法检测ECU4100a是通过非法帧检测部130进行非法的消息的检测的状态。

[0291] 如果由通信开始/结束检测部4283检测到与外部的通信的结束(次序S4102),则头单元4200判断从车辆的使用开始起是否经过了一定时间(次序S4103)。在从车辆的使用开始起没有经过一定时间的情况下,由于不能向待机模式转移,所以不发送指示向待机模式的转移的触发帧(即,将次序S4104、S4105跳过)。

[0292] 在从车辆的使用开始起经过了一定时间的情况下,头单元4200判断是否检测到非法的消息(次序S4104)。在将指示向检查模式的转移的触发帧发送之后检测到非法的消息的情况下,由于不能向待机模式转移,所以不发送指示向待机模式的转移的触发帧(即,将次序S4105跳过)。

[0293] 在次序S4104中判断为没有检测到非法的消息的情况下,头单元4200指示向待机模式的转移(步骤S4105)。具体而言,头单元4200发送指示向待机模式的转移的触发帧。

[0294] 从头单元4200发送到总线500c的、指示向待机模式的转移的触发帧由网关300向总线500a、500b转送。

[0295] 非法检测ECU4100a将发送到总线500a的触发帧接收,将动作模式向待机模式转移(次序S4106)。从此时起,非法检测ECU4100a不再进行由非法帧检测部130实施的非法的消息的检测。

[0296] 这里,着眼于非法检测ECU中的非法检测ECU4100a进行了说明,但例如关于非法检测ECU4100b也同样,能够对应于在次序S4105中发送的触发帧,将动作模式设为待机模式。

[0297] [4.6有关向待机模式的转移的次序(从车辆的使用开始起经过一定时间时)]

[0298] 以下,对从开始车辆的使用起经过了一定时间的情况下的头单元4200及非法检测ECU4100a的动作进行说明。

[0299] 图39是表示头单元4200检测到从车辆的使用开始起经过了一定时间、向非法检测

ECU4100a指示向待机模式的转移、非法检测ECU4100a向待机模式转移的动作例的次序图。

[0300] 在该动作例的开始阶段,非法检测ECU4100a为检查模式(次序S4201)。例如,是作为在该阶段以前非法检测ECU4100a接受到头单元4200在检测到车辆的使用开始时指示向检查模式的转移的触发帧的结果成为检查模式的状态。此时,非法检测ECU4100a是通过非法帧检测部130进行非法的消息的检测的状态。

[0301] 如果由车使用开始检测部4282检测到从开始车辆的使用起经过了一定时间(次序S4202),则头单元4200判断是否是和外部的通信中(次序S4203)。在与外部通信的情况下,由于不能向待机模式转移,所以不发送指示向待机模式的转移的触发帧(即,将次序S4204、S4205跳过)。

[0302] 在不是与外部通信中的情况下,头单元4200判断是否检测到非法的消息(次序S4204)。在发送指示向检查模式的转移的触发帧之后检测到非法的消息的情况下,由于不能向待机模式转移,所以不发送指示向待机模式的转移的触发帧(即,将次序S4205跳过)。

[0303] 在次序S4204中判断为没有检测到非法的消息的情况下,头单元4200指示向待机模式的转移(次序S4205)。具体而言,头单元4200发送指示向待机模式的转移的触发帧。

[0304] 从头单元4200发送到总线500c的、指示向待机模式的转移的触发帧由网关300向总线500a、500b转送。

[0305] 非法检测ECU4100a将发送到总线500a的触发帧接收,将动作模式向待机模式转移(次序S4206)。从此时起,非法检测ECU4100a不再进行由非法帧检测部130实施的非法的消息的检测。

[0306] 这里,着眼于非法检测ECU中的非法检测ECU4100a进行了说明,但例如关于非法检测ECU4100b也同样,能够对应于在次序S4205中发送的触发帧,将动作模式设为待机模式。

[0307] [4.7实施方式4的效果]

[0308] 在车载网络系统13中,根据车辆的状态,非法检测ECU4100a、4100b将动作模式在进行非法的消息的检测的检查模式和不进行非法的消息的检测的待机模式之间进行切换。由此,通过根据车辆的状态、仅在需要的情况下进行非法的消息的检测,能够抑制电力消耗量。此外,非法检测ECU4100a、4100b即使不具有直接检测车辆的状态的机构,也能够通过来自头单元4200的触发帧得到切换动作模式的定时。

[0309] (其他实施方式等)

[0310] 如以上这样,作为有关本发明的技术的例示而说明了实施方式1~4。但是,有关本发明的技术并不限于此,对于适当进行了变更、替换、附加、省略等的实施方式也能够应用。例如,以下这样的变形例也包含在本发明的一实施方式中。

[0311] (1)在上述实施方式中,表示了由ECU400a~400d或ECU3400a~3400d定期地发送帧的例子,但帧也可以作为通知状态变化的事件来发送。例如,ECU也可以不是定期地发送门的开闭状态,而仅在门的开闭状态变化的情况下发送帧。此外,ECU也可以将帧定期地发送,并在发生状态变化时发送。

[0312] (2)在实施方式3中,表示了根据数据值和计数器值计算MAC的例子,但也可以仅根据数据值计算MAC。此外,也可以仅根据计数器值计算MAC。此外,帧中包含的MAC的尺寸并不限制为4bytes,也可以是按每次发送而不同的尺寸。同样,时速等的数据值的尺寸及计数器值的尺寸也并不限制为1byte。此外,也可以并不一定在帧中包含计数器值。

[0313] (3) 在实施方式3中,表示了将计数器值按每次发送递增的例子,但计数器值也可以是根据时刻而自动递增的值。此外,也可以将时刻本身的值作为计数器的替代来使用。即,如果基于每当发送数据帧时变化的变量(计数器、时刻等)生成MAC,则能够使MAC的非法的解读困难化。此外,在实施方式3中,非法检测ECU的MAC生成部3170根据消息ID、数据字段的开头1byte和计数器保持部3190的计数器值计算MAC值。代之,也可以根据消息ID、数据字段的开头1byte、和作为数据字段的下个1byte的计数器值计算MAC值。此外,也可以将计数器保持部3190的计数器值更新,以使其与被判定是非法的数据字段中的计数器值匹配。

[0314] (4) 在上述实施方式中,将CAN协议的数据帧用标准ID格式记述,但也可以是扩展ID格式。在扩展ID格式的情况下,由于将标准ID格式中的ID位置的基础ID和扩展ID加起来用29位表示ID(消息ID),所以只要将该29位的ID作为上述实施方式中的ID(消息ID)就可以。

[0315] (5) 在上述实施方式中,设MAC计算的算法为HMAC,但它也可以是CBC—MAC(Cipher Block Chaining Message Authentication Code)、CMAC((Cipher—based MAC)。此外,关于在MAC计算中使用的填充,可以是零填充、ISO10126、PKCS#1、PKCS#5、PKCS#7,此外,只要是块的数据尺寸为计算所需要的填充的方式,什么方式都可以。此外,关于4bytes等对块的尺寸的变更方法,也可以对开头、最末尾、中间的任何部分进行填充。此外,在MAC计算中使用的数据也可以不是连续的数据(例如4bytes的连续数据),也可以是按照特定的规则每次1bit地收集而结合的数据。

[0316] (6) 在上述实施方式中表示的CAN协议也可以具有还包含TTCAN(Time—Triggered CAN)、CANFD(CAN with Flexible Data Rate)等的派生性的协议的广义的意义。

[0317] (7) 在上述实施方式中,例示了在总线上连接着非法的ECU的例子,但也有可能是ECU400a~400d或ECU3400a~3400d那样的已有的ECU因某些原因而作为非法的ECU工作。即使在该情况下,通过如上述实施方式所示那样非法检测ECU适当地检测非法的帧并发送错误帧,也能够阻止其他ECU处理非法的帧。

[0318] (8) 在实施方式2中,使用将消息ID与被容许的数据范围建立了对应的数据范围列表,根据接收到的数据帧的数据是否包含在按每个消息ID而被容许的数据范围中,来进行是否非法的判定,但也可以在数据范围列表中不包含消息ID,而设定对于全部的消息ID共通地容许的数据范围(例如“0~180”),不论消息ID如何都进行是否非法的判定。此外,非法检测ECU保持的数据范围列表也可以为将在连接着该非法检测ECU的总线中可能发送的消息ID与数据范围建立了对应的列表。由此,数据范围列表也能够作为在实施方式1中表示的正规ID列表使用。也可以利用它在实施方式2所表示的非法检测ECU中也进行在实施方式1中表示的消息ID的检查(次序S1004)。

[0319] (9) 也可以代替在实施方式2中表示的将消息ID与被容许的数据范围建立了对应的数据范围列表,而非法检测ECU使用将消息ID与被容许的数据长建立了对应的数据长列表。在此情况下,非法检测ECU判定接收到的数据帧的控制字段的值是否与表示非法的规定条件相符。该表示非法的规定条件是控制字段中的数据长(DLC)不是在数据长列表中与消息ID建立了对应的数据长的条件。非法检测ECU根据接收到的DCL是否是在数据长列表中按每个消息ID被容许的数据长,来进行是否为非法的判定。

[0320] (10) 在上述实施方式中,特别着眼于数据帧进行了说明,但关于远程帧,非法检测

ECU也能够检测一定的非法。例如,非法检测ECU也可以使用在实施方式1中表示的正规ID列表来判定接收到的远程帧中的消息ID是否为非法。此外,非法检测ECU也可以使用上述数据长列表,根据接收到的远程帧中的控制字段的数据长(DLC)是否是按每个消息ID被容许的数据长,来判定是否是非法。此外,在上述实施方式中表示的、在非法检测ECU通过接收非法的帧而进行了非法的检测的情况下发送的错误帧优选的是在非法的检测后迅速地发送。另外,非法检测ECU在非法的检测后,该非法的帧的CRC序列的最末尾被发送之前发送错误帧是有用的。由此,其他ECU通过错误帧的检测或CRC的检查中的错误检测,将该非法的帧的处理中止。另外,远程帧也与数据帧同样,包括消息ID、控制字段及CRC序列。

[0321] (11) 在上述实施方式中,表示了非法检测ECU在一定条件下发送错误显示消息,但也可以不发送错误显示消息。在此情况下,网关及头单元等的ECU不再特别需要保持与非法检测ECU对应的结构(用来接收错误显示消息的接收ID列表等)。另外,非法检测ECU既可以代替错误显示消息的发送而在自己具备扬声器或显示器等的情况下自己报告错误,也可以将错误的日志记录到存储介质等中。

[0322] (12) 在实施方式4所表示的车载网络系统13中,能够切换动作模式的非法检测ECU和不切换动作模式的非法检测ECU(即与常时检查模式同样的非法检测ECU)也可以混合存在。此外,非法检测ECU除了检测在总线上发送的非法的消息的功能以外,也可以与其他ECU同样还具有根据不非法的消息执行预先设定的处理的功能、或执行车辆的状态的检测或车辆的控制等的处理的功能。在动作模式是不进行特定的非法检测的待机模式的情况下,除了电力消耗的降低以外,还可能发生非法检测ECU的处理负荷的减少及总线中的通信量降低等的效果。

[0323] (13) 在实施方式4中,头单元4200具有在车辆的状态满足一定条件的情况下发送触发帧的功能,但也可以是其他ECU具有该功能。在该车辆的状态满足一定状态的情况下发送触发帧的功能既可以是车载网络系统13中的1台ECU具有,也可以是多个ECU(既可以是全部ECU,也可以是一部分的ECU)具有。即,也可以使其他ECU(ECU400a等)包含实施方式4所表示的头单元4200的非法帧检测部4280、模式变更指示部4281、车使用开始检测部4282及通信开始/结束检测部4283。图40是将ECU400a一部分变形、包含非法帧检测部4280、模式变更指示部4281、车使用开始检测部4282及通信开始/结束检测部4283而成的ECU4400的结构图。图40所示的ECU4400中的帧解释部4450是将在实施方式1中表示的帧解释部450变形一部分而得到的结构。帧解释部4450除了向帧处理部410、帧生成部4420及接收ID判断部430的数据转送以外,向非法帧检测部4280、车使用开始检测部4282及通信开始/结束检测部4283也转送接收到的帧。该转送既可以是全部的接收到的帧的转送,也可以是仅与各检测部关联的帧的转送。非法帧检测部4280进行与实施方式4的非法帧检测部4280相同的动作。车使用开始检测部4282及通信开始/结束检测部4283根据ECU4400接收到的帧,检测车体被开始使用、通信开始、通信结束等。例如,也可以是头单元4200或具有与外部的通信功能的ECU发送对通信的开始或结束进行通知的帧,通信开始/结束检测部4283对应于该帧的接收而检测通信的开始或通信的结束。模式变更指示部4281与实施方式4的功能是同样的。帧生成部4420具有实施方式1的帧生成部420的功能。帧生成部4420还具有按照来自模式变更指示部4281的用于模式变更的触发帧的发送委托来构成触发帧、将触发帧向帧收发部270通知而使其发送的功能。该ECU4400执行与在图37的次序S4002~S4005中表示的处理顺序、在

图38的次序S4102~S4105中表示的处理顺序及在图39的次序S4202~S4205中表示的处理顺序同样的处理顺序。在该车辆的状态满足一定状态的情况下发送触发帧的功能也可以由非法检测ECU具有。

[0324] (14) 在实施方式4中表示的由头单元4200进行的是否应指示向待机模式的转移的判断(参照图38、图39)只不过是有效的判断的一例,也可以是其他的判断。例如,也可以单单在检测到通信结束的情况下进行向待机模式的转移的指示,此外,也可以在从车辆的使用开始起经过了规定时间的情况下进行向待机模式的转移的指示。该规定时间既可以是例如几分钟等的一定时间,并且也可以是在车辆的使用开始后到在总线上进行一定数量的消息的发送为止所需要的时间、在使用开始后到执行一定的处理顺序为止所需要的时间。此外,也可以单单在总线上在一定期间中没有检测到非法的消息的情况下进行向待机模式的转移的指示。即,为了根据车辆的状态将非法检测ECU的动作模式变更为检查模式或待机模式,只要基于实验、理论等是有用的,则可以基于任意的判断材料利用任意的判断方法(判断算法等)。例如,头单元4200也可以并不一定包含车使用开始检测部4282及通信开始/结束检测部4283这两者,也可以仅包含某一方,也可以包含用来检测其他车辆的状态的检测部。作为检测部,例如可以举出是否是停车中的检测部、是否是刹车中的检测部、门的开闭的检测部、加油口的开闭的检测部、是否是充电中的检测部、是否是行驶中的检测部、向座椅的就座的检测部、乘车中的检测部、乘车完成的检测部、下车中的检测部等。车载网络系统只要如以下这样构成就可以:在检测到车辆的状态满足一定条件的情况下,将非法检测ECU的动作模式在进行对总线上的非法的消息进行检测的规定种类的检测处理的第1模式(检查模式)、和不进行该检测处理的第2模式(待机模式等)之间进行切换。此外,除了在第2模式中完全不进行非法的消息的检测处理的方式以外,也可以采用在第2模式中,虽然不进行该规定种类的检测处理、但执行处理量比该规定种类的检测处理少的某种非法的消息的检测处理的方式。此外,也可以是,头单元4200具备非法检测ECU的动作模式变更用按钮及其他用户接口,根据用户对该用户接口的操作、输入等,向非法检测ECU指示动作模式的变更。作为其用户接口,除了物理性的按钮以外,也可以是显示在触摸面板等上的按钮等,也可以使用声音输入机构。另外,也可以在由车使用开始检测部4282、通信开始/结束检测部4283等检测部检测到车辆的状态的变化时,通过画面显示、声音输出等向用户询问是否需要动作模式的变更。也可以是,头单元4200如果受理了作为来自用户的应答的有关是否需要动作模式的变更的输入,则在该输入表示需要动作模式的切换时向非法检测ECU指示动作模式的变更。例如,头单元4200可以在从车辆的使用开始起经过了一定时间时向用户询问是否转移为待机模式,对此用户可以选择继续检查模式。此外,也可以是,头单元4200只是仅将车辆的使用开始、通信开始、通信结束等事件的信息向非法检测ECU4100a等通知,关于应转移为哪个动作模式,由非法检测ECU4100a等判断。

[0325] (15) 在实施方式4中表示的非法检测ECU4100a包括实施方式1的非法检测ECU100a的功能,但非法检测ECU的非法应对方法的具体的实现方式也可以是在实施方式2、3中表示的方式。即,也可以使车载网络系统13中的各非法检测ECU(非法检测ECU4100a等)为例如图41所示包含实施方式2的非法检测ECU2100a的功能的非法检测ECU5100。此外,也可以使非法检测ECU4100a等为如图42所示包含实施方式3的非法检测ECU3100a的功能的非法检测ECU6100。另外,图41所示的非法检测ECU5100及图42所示的非法检测ECU6100都与非法检测

ECU4100a同样包括帧解释部4150、触发帧检测部4170、模式保持部4180。此外,非法检测ECU4100a也可以构成为能够将在实施方式1~3的各自中表示的非法检测的处理顺序的两个以上切换并执行。例如也可以是,非法检测ECU通过动作模式对为了检测非法的消息而处理量比较多的在实施方式2或3中表示的非法检测的处理顺序、和处理量比较少的在实施方式1中表示的非法检测的处理顺序进行切换。在此情况下,动作模式被在例如进行处理量比较多的检测处理的第1模式、与不进行处理量比较多的检测处理而进行处理量比较少的检测处理的第2模式之间切换。

[0326] (16)在上述实施方式中表示的非法帧检测部及非法MAC检测部也可以安装到称作CAN控制器的硬件、或在与CAN控制器连接而动作的处理器上动作的固件中。此外,MAC密钥保持部、计数器保持部、正规ID列表保持部、数据范围列表保持部可以保存在称作CAN控制器的硬件的寄存器、或在与CAN控制器连接而动作的处理器上动作的固件中。

[0327] (17)上述实施方式的各ECU(包括网关及头单元)例如是包括处理器、存储器等的数字电路、模拟电路、通信电路等的装置,但也可以包括硬盘装置、显示器、键盘、鼠标等其他硬件构成要素。此外,也可以代替存储在存储器中的控制程序被处理器执行而软件性地实现功能,而由专用的硬件(数字电路等)实现其功能。

[0328] (18)构成上述实施方式的各装置的构成要素的一部分或全部也可以由1个系统LSI(Large Scale Integration:大规模集成电路)构成。系统LSI是将多个构成部集成到1个芯片上而制造的超多功能LSI,具体而言,是包括微处理器、ROM、RAM等而构成的计算机系统。在上述RAM中记录有计算机程序。通过由上述微处理器按照上述计算机程序动作,系统LSI实现其功能。此外,构成上述各装置的构成要素的各部既可以单独地形成1个芯片,也可以包含一部分或全部而形成1个芯片。此外,这里设为系统LSI,但根据集成度的差异,也有称作IC、LSI、超级LSI、超大规模LSI的情况。此外,集成电路化的方法并不限于LSI,也可以由专用电路或通用处理器实现。也可以利用在LSI制造后能够编程的FPGA(Field Programmable Gate Array)或能够重构LSI内部的电路单元的连接及设定的可重构处理器。进而,如果因半导体技术的进步或派生的其他技术而出现替代LSI的集成电路化的技术,则当然也可以使用该技术进行功能块的集成化。有可能是生物技术的应用等。

[0329] (19)构成上述各装置的构成要素的一部分或全部也可以由对于各装置可拆装的IC卡或单体的模块构成。上述IC卡或上述模块是由微处理器、ROM、RAM等构成的计算机系统。上述IC卡或上述模组也可以包括上述超多功能LSI。通过由微处理器按照计算机程序动作,上述IC卡或上述模块实现其功能。该IC卡或该模块也可以具有耐篡改性。

[0330] (20)作为本发明的一形态,也可以是上述所示的非法检测方法、非法应对方法等方法。此外,也可以是通过计算机实现这些方法的计算机程序,也可以是由上述计算机程序构成的数字信号。此外,作为本发明的一形态,也可以是将上述计算机程序或上述数字信号记录到计算机可读的记录介质,例如软盘、硬盘、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、BD(Blu-ray(注册商标)Disc)、半导体存储器等中的形态。此外,也可以是记录在这些记录介质中的上述数字信号。此外,作为本发明的一形态,也可以是将上述计算机程序或上述数字信号经由电气通信线路、无线或有线通信线路、以因特网为代表的网络、数据广播等传送的形态。此外,作为本发明的一形态,也可以是具备微处理器和存储器的计算机系统,上述存储器记录有上述计算机程序,上述微处理器按照上述计算机程序动作。此外,也可以通过

将上述程序或上述数字信号记录到上述记录介质中并移送、或通过将上述程序或上述数字信号经由上述网络等移送,来由独立的其他计算机系统实施。

[0331] (21) 通过将在上述实施方式及上述变形例中表示的各构成要素及功能任意地组合而实现的形态也包含在本发明的范围中。

[0332] 工业实用性

[0333] 本发明可以为了在车载网络系统中有效地抑制由非法的ECU带来的影响而利用。

[0334] 标号说明

[0335] 10、11、12、13 车载网络系统

[0336] 100a、100b、2100a、2100b、3100a、3100b、4100a、4100b、5100、6100 非法检测电子控制单元(非法检测ECU)

[0337] 110 非法检测计数器保持部

[0338] 120 正规ID列表保持部

[0339] 130、2130 非法帧检测部

[0340] 140、230、320、420、3420、4230、4420 帧生成部

[0341] 150、260、350、450、2150、3150、4150、4260、4450 帧解释部

[0342] 160、270、360、460 帧收发部

[0343] 200、4200 头单元

[0344] 210 显示控制部

[0345] 220、410 帧处理部

[0346] 240、330、430 接收ID判断部

[0347] 250、340、440 接收ID列表保持部

[0348] 300 网关

[0349] 310 转送处理部

[0350] 370 转送规则保持部

[0351] 400a、400b、400c、400d、3400a、3400b、3400c、3400d、4400 电子控制单元(ECU)

[0352] 401 发动机

[0353] 402 制动器

[0354] 403 门开闭传感器

[0355] 404 窗开闭传感器

[0356] 470 数据取得部

[0357] 500a、500b、500c 总线

[0358] 2120 数据范围列表保持部

[0359] 3130 非法MAC检测部

[0360] 3410、3170MAC 生成部

[0361] 3430、3180MAC 密钥保持部

[0362] 3440、3190 计数器保持部

[0363] 4170 触发帧检测部

[0364] 4180 模式保持部

[0365] 4280 非法帧检测部

- [0366] 4281 模式变更指示部
- [0367] 4282 车使用开始检测部
- [0368] 4283 通信开始/结束检测部

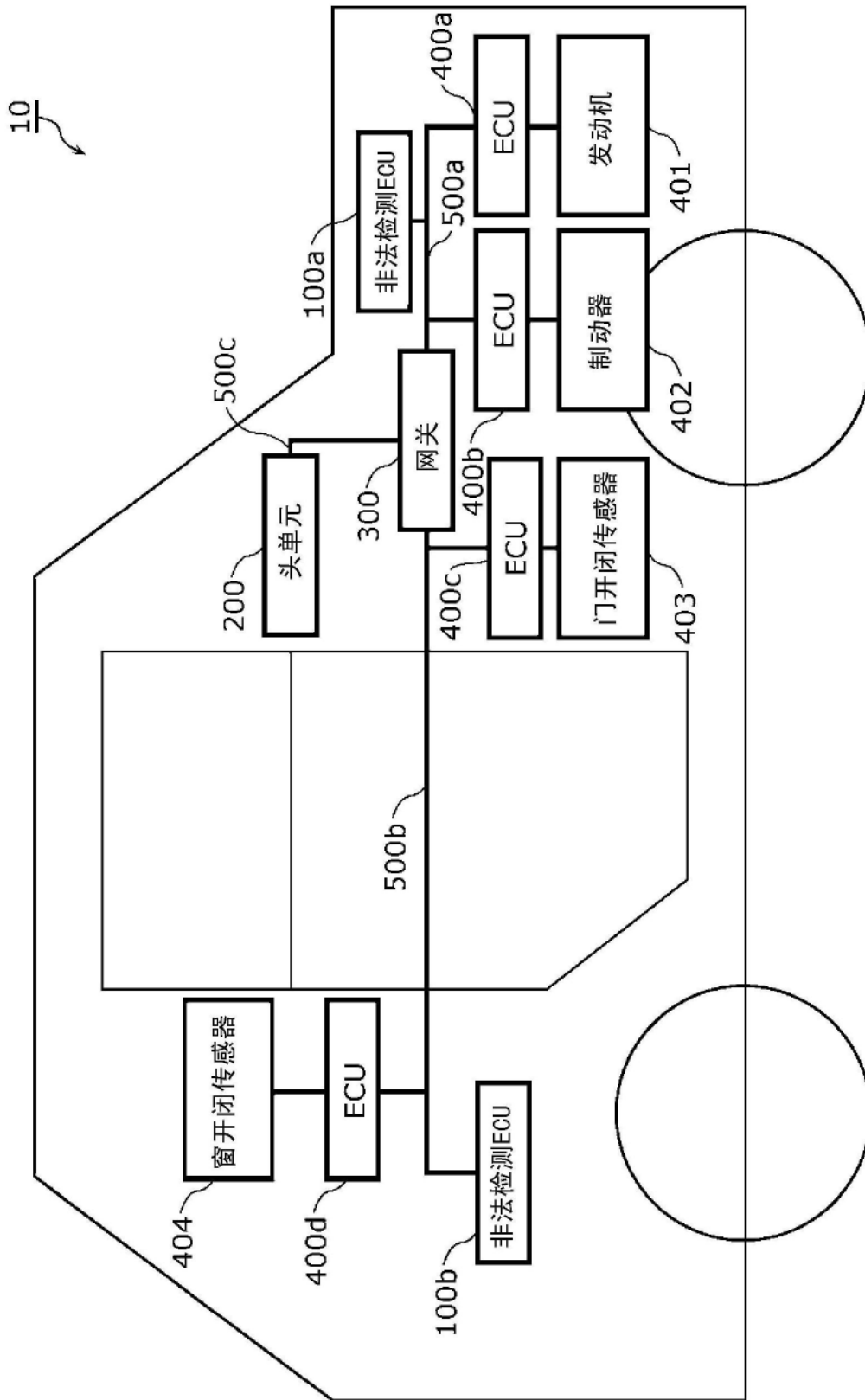


图1



图2

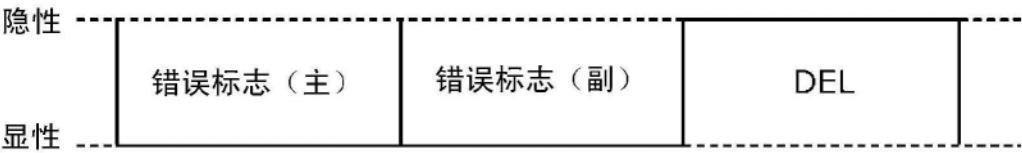


图3

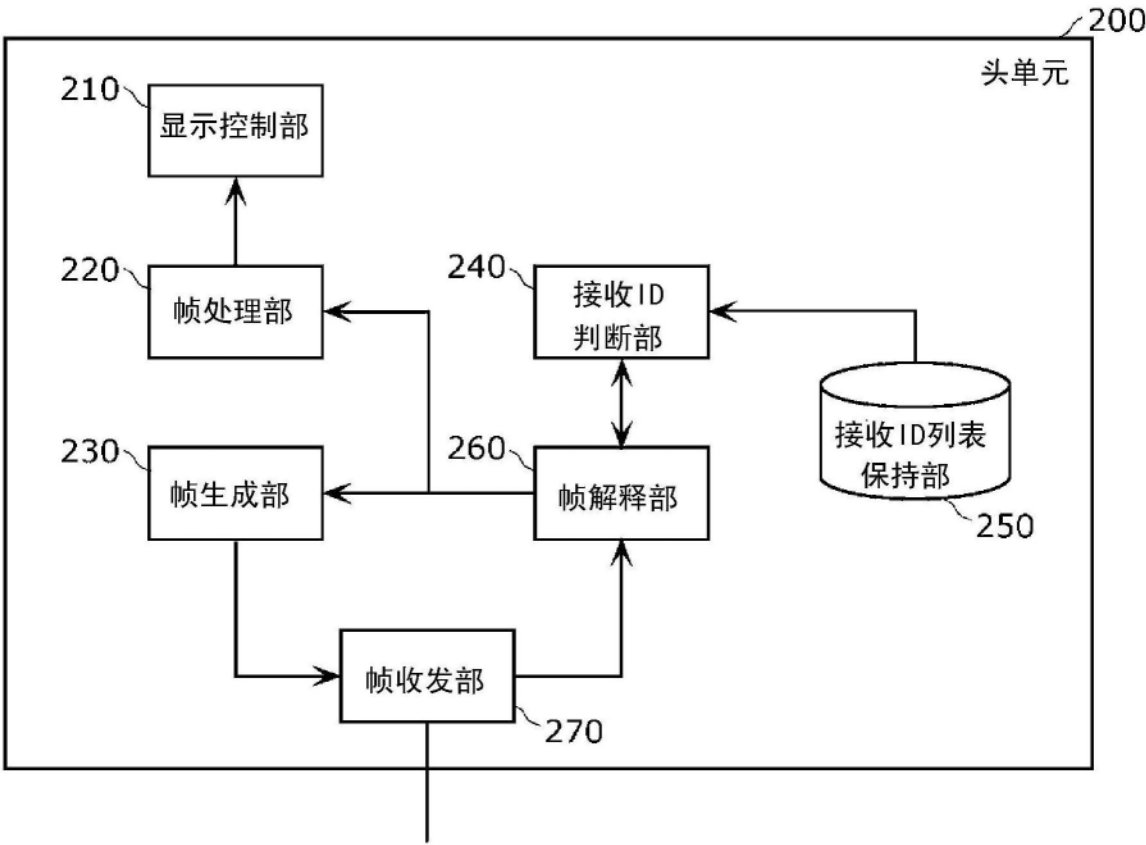


图4

接收ID列表
1
2
3
4

图5

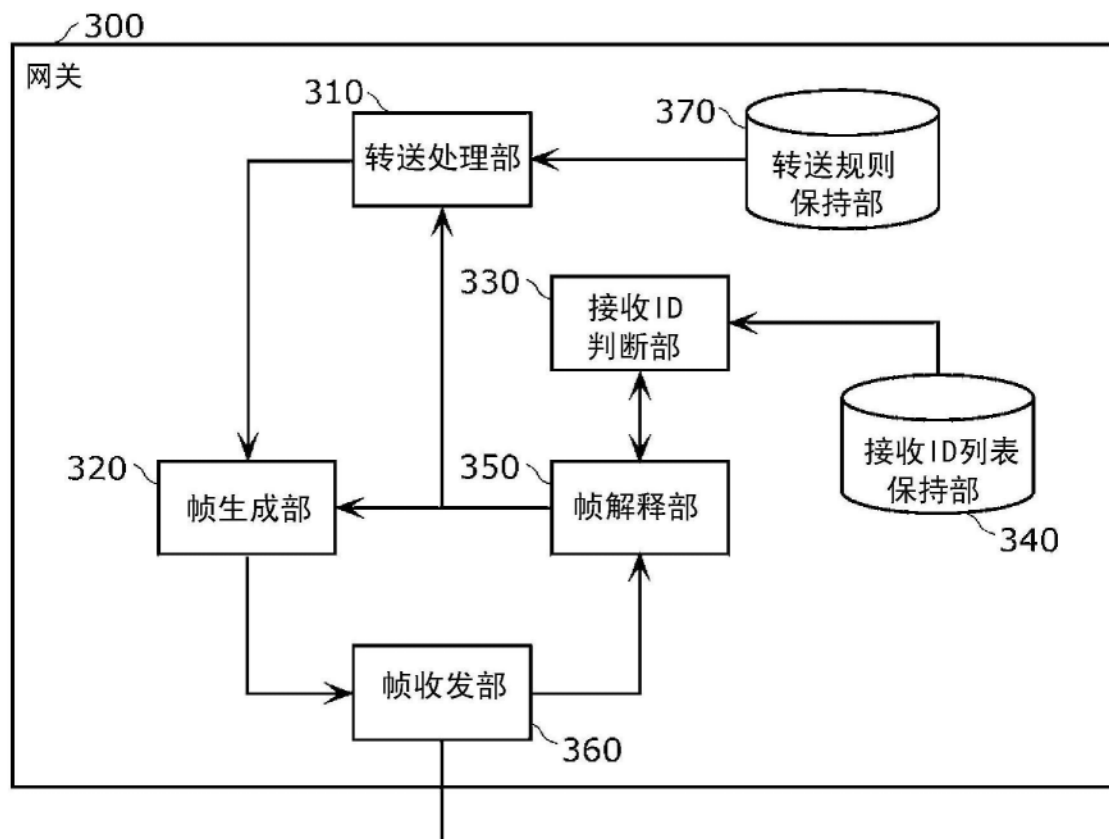


图6

转送规则

转送源	转送目的地	ID
500a	500b	*
500a	500c	*
500b	500a	3
500b	500c	*
500c	500a	-
500c	500b	-

图7

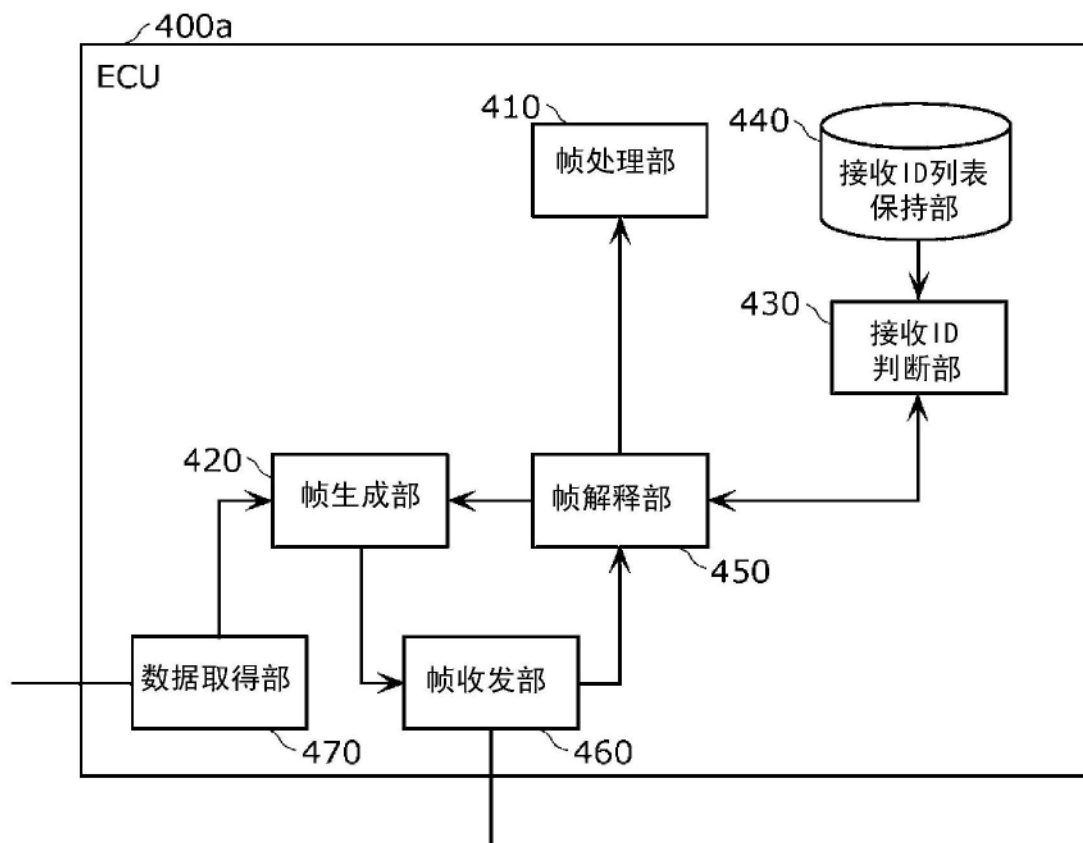


图8

接收ID列表
1
2
3

图9

ID	数据
1	0
1	1
1	2
1	3
1	4
...	...

图10

ID	数据
2	100
2	90
2	80
2	70
2	60
...	...

图11

ID	数据
3	1
3	1
3	0
3	0
3	0
...	...

图12

ID	数据
4	0
4	10
4	20
4	30
4	40
...	...

图13

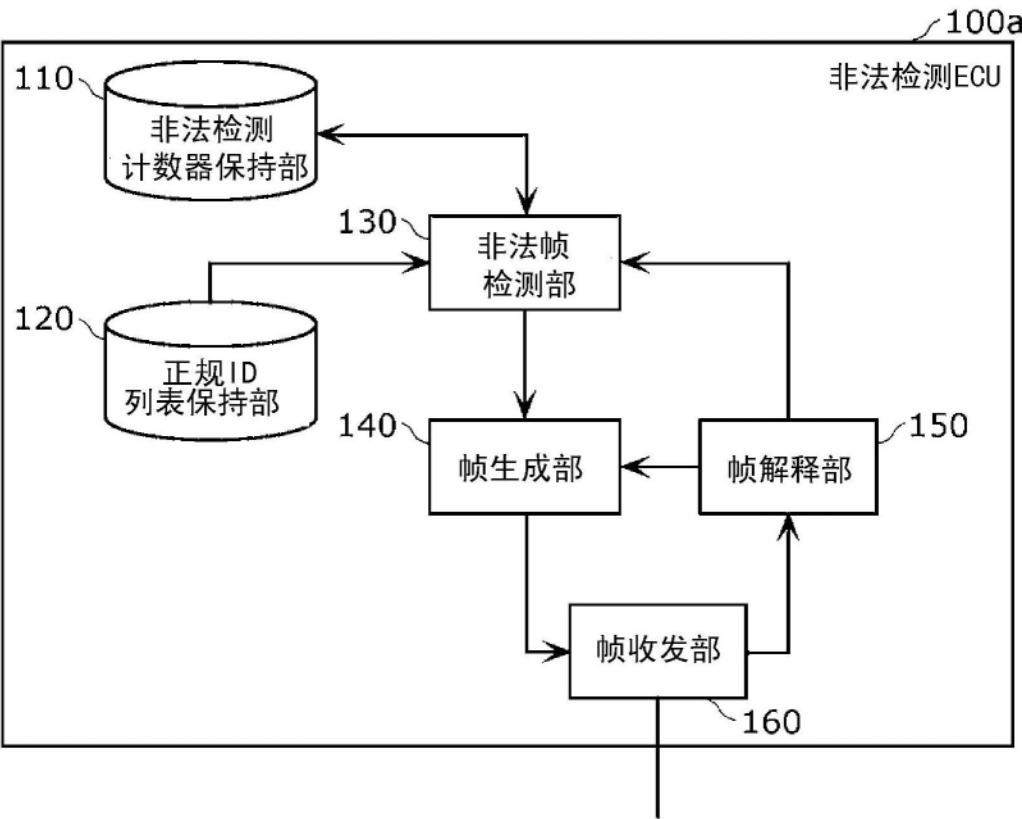


图14

正规ID列表
1
2
3

图15

正规ID列表
1
2
3
4

图16

ID	非法检测计数器
1	0
2	0
3	0
4	1
5	0
...	...

图17

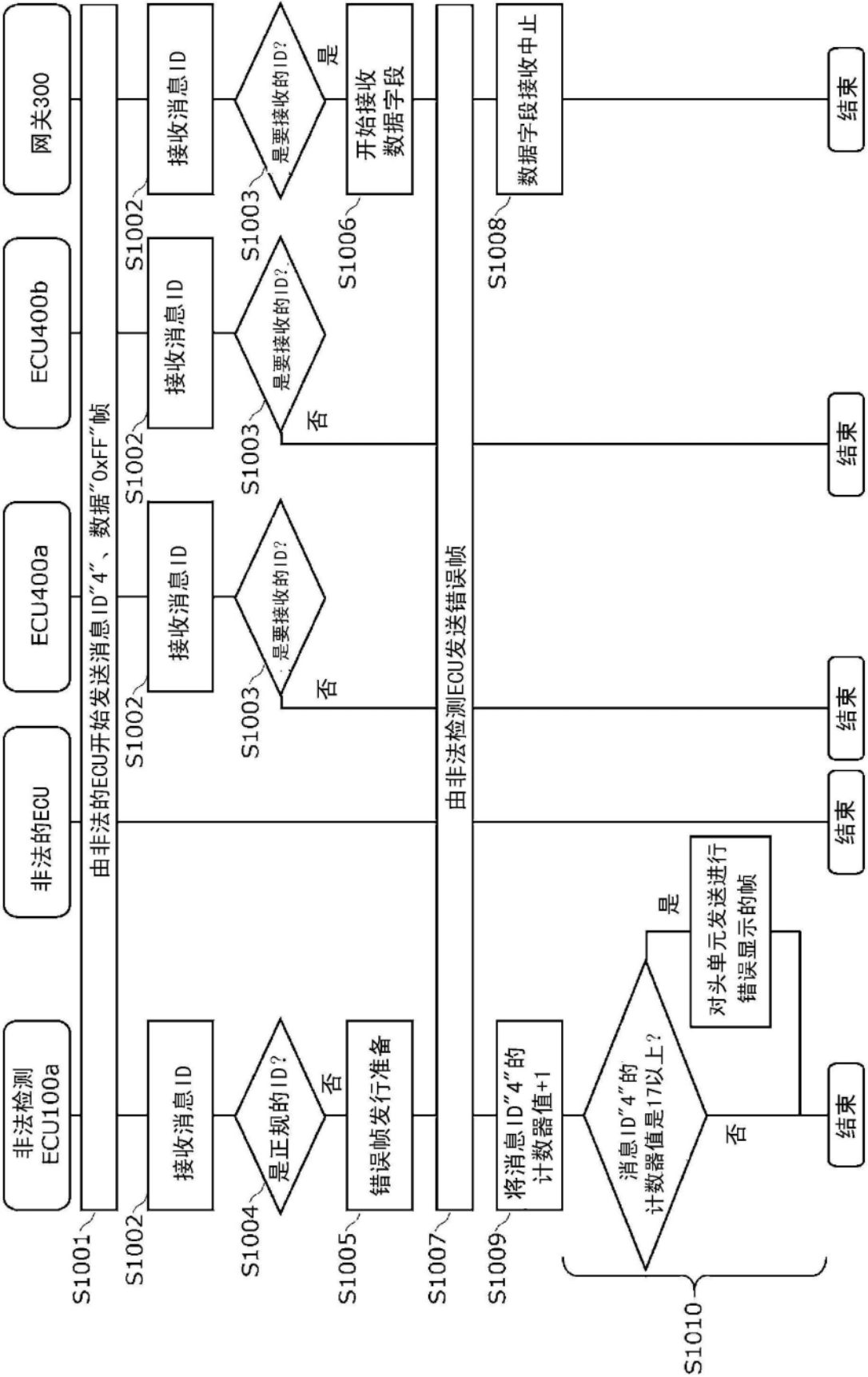


图18

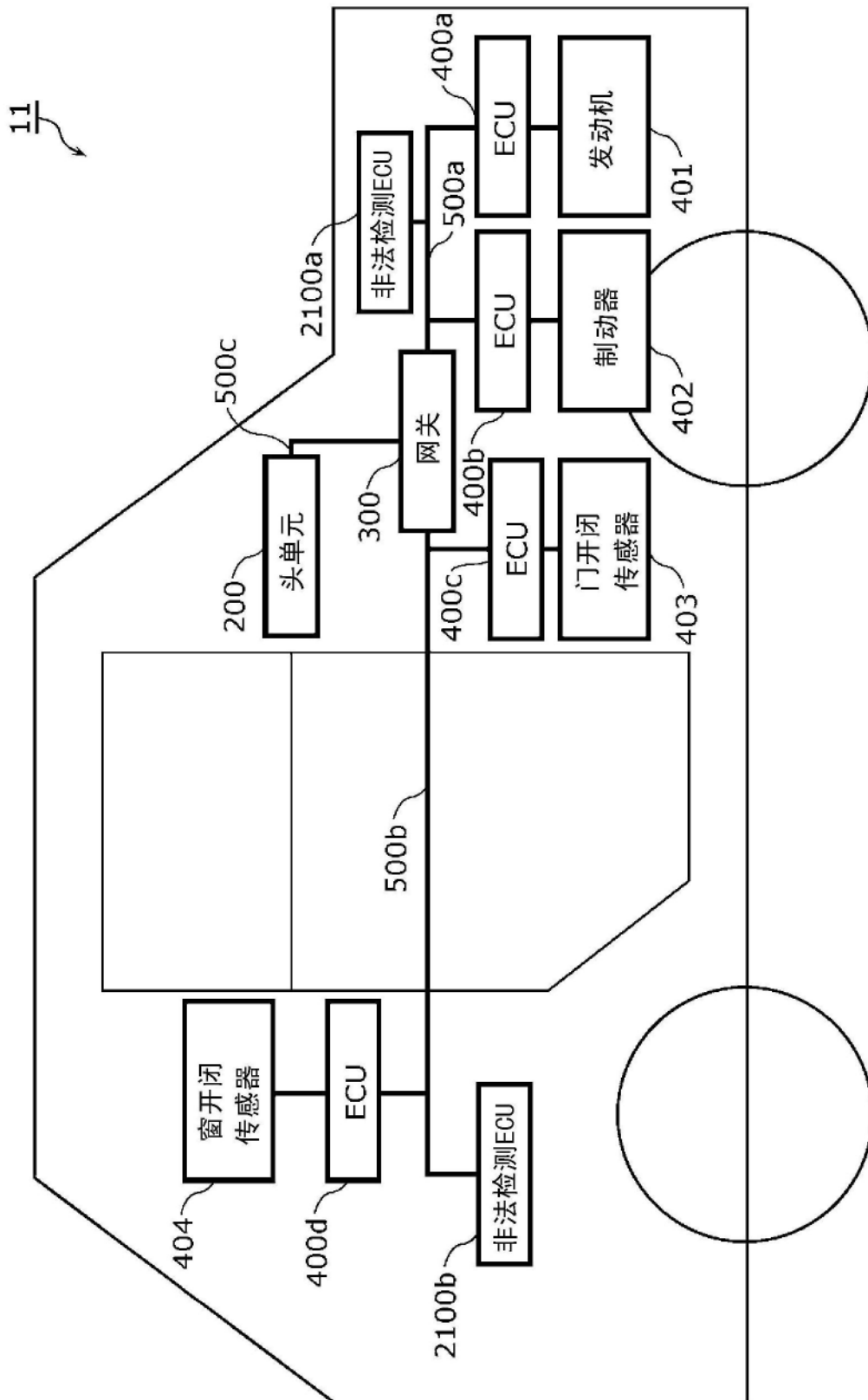


图19

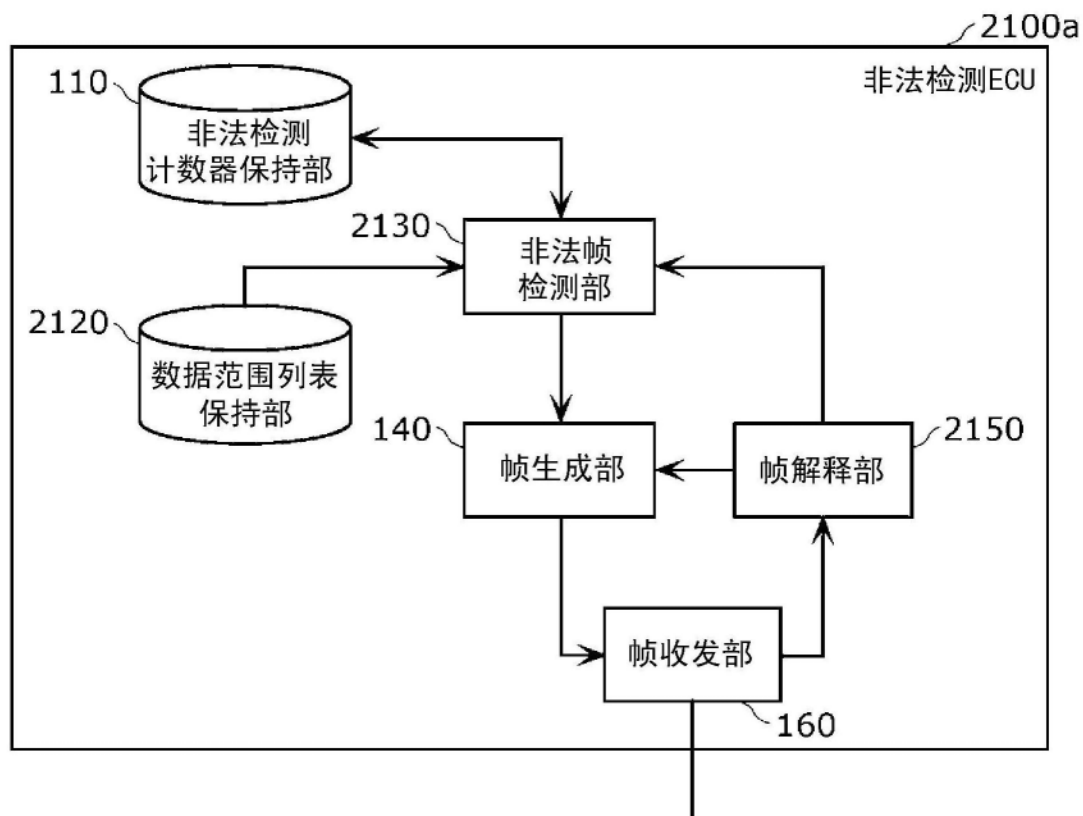


图20

ID	数据范围
1	0~180
2	0~100
3	0, 1
4	0~100
...	...

图21

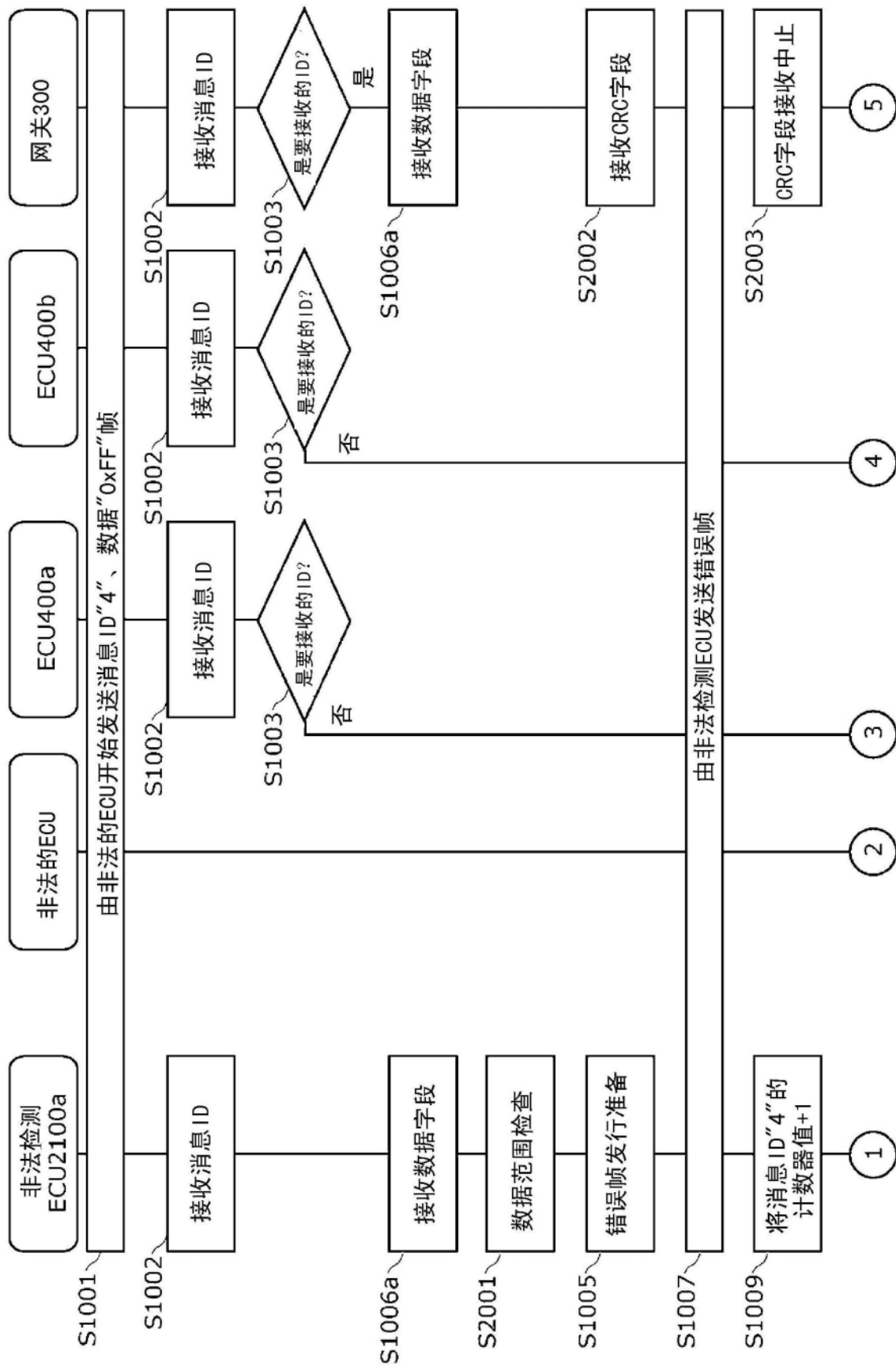


图22

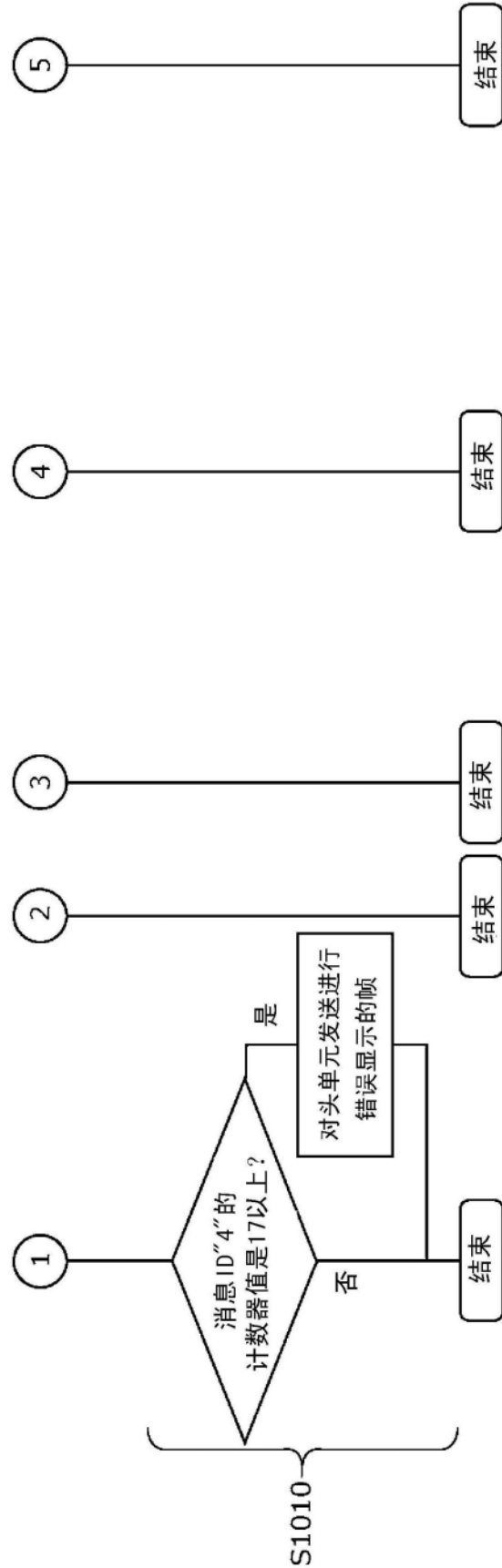


图23

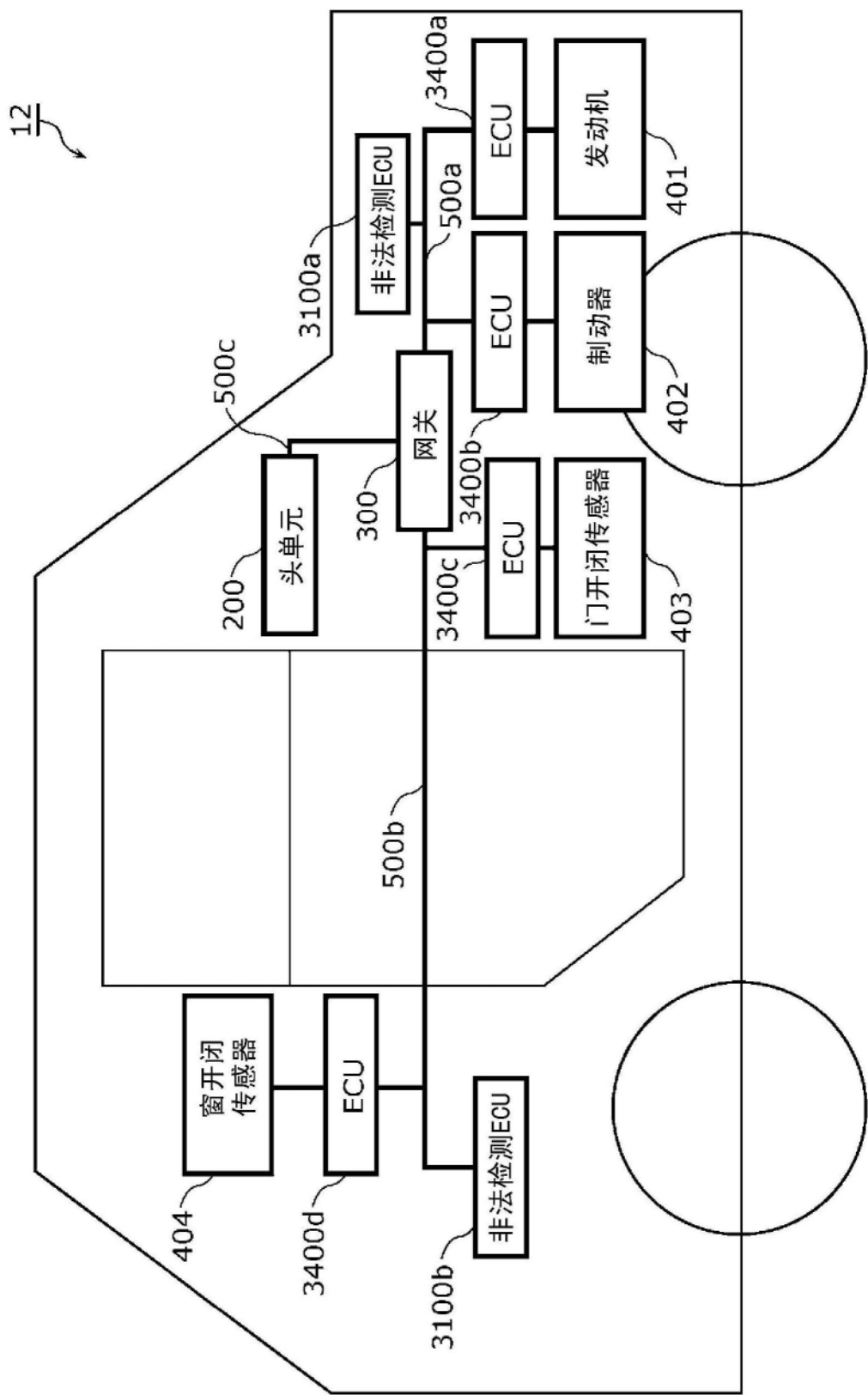


图24

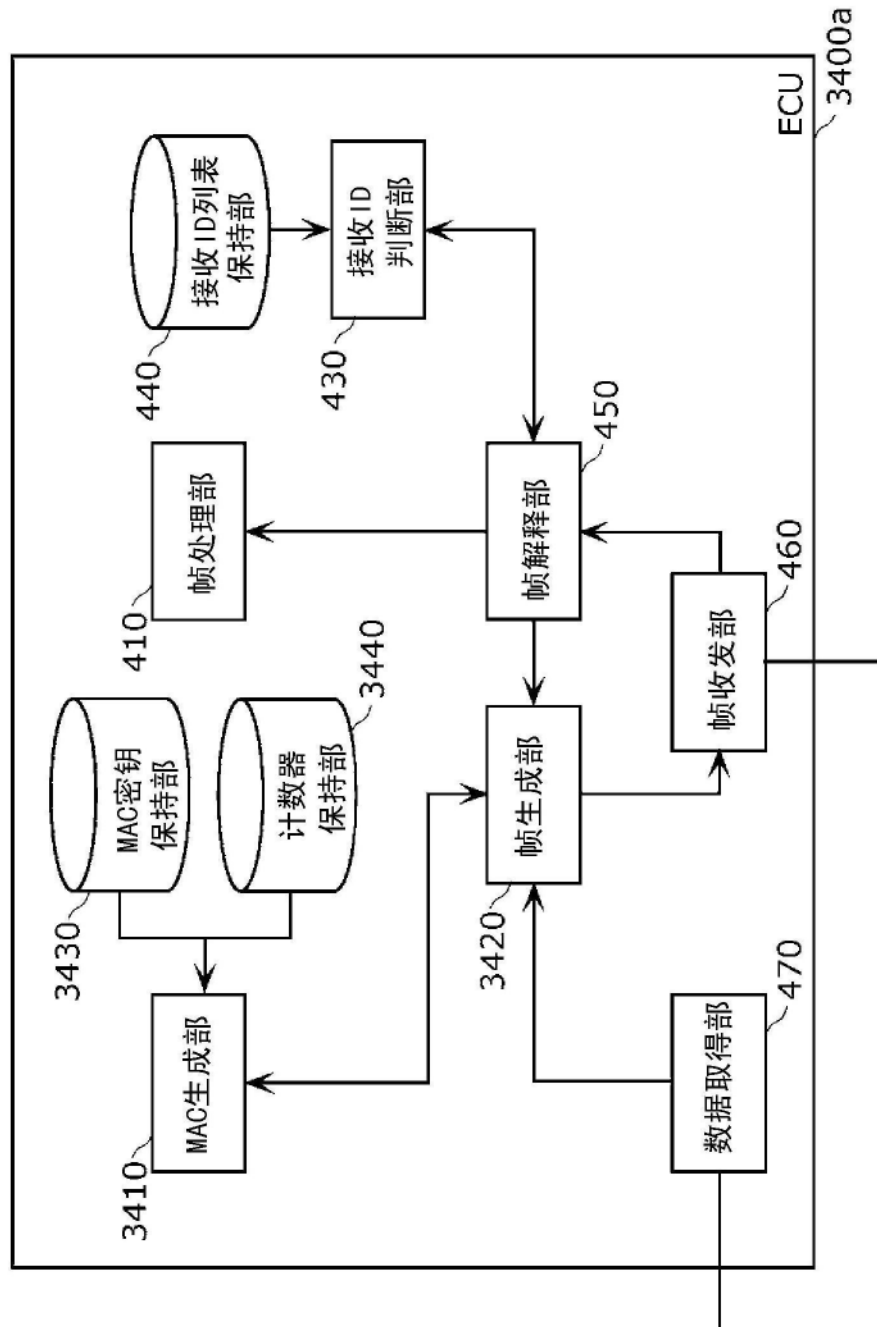


图25

ID	数据
1	0 1 0x1a c4 f7 d3
1	1 2 0xf9 3b 65 9e
1	2 3 0x34 5c ef 79
1	3 4 0x90 2a e3 dd
1	4 5 0x31 2c d5 ee
...	...

图26

ID	数据
2	100 1 0x34 5d ef 78
2	90 2 0x34 2d d5 ea
2	80 3 0x90 8a e8 6b
2	70 4 0x4a d4 f7 d8
2	60 5 0xf1 32 7e 6a
...	...

图27

ID	数据
3	1 1 0x92 d5 e8 3b
3	1 2 0x81 a2 c5 ca
3	0 3 0xf8 4d 66 9a
3	0 4 0x95 a2 3e ac
3	0 5 0x1b c5 f6 d1
...	...

图28

ID	数据
4	0 1 0x9d 20 03 d3
4	10 2 0x3a 2d 5b ef
4	20 3 0x4c c8 3b b5
4	30 4 0x5f f1 d2 da
4	40 5 0xb1 0b 70 a4
...	...

图29

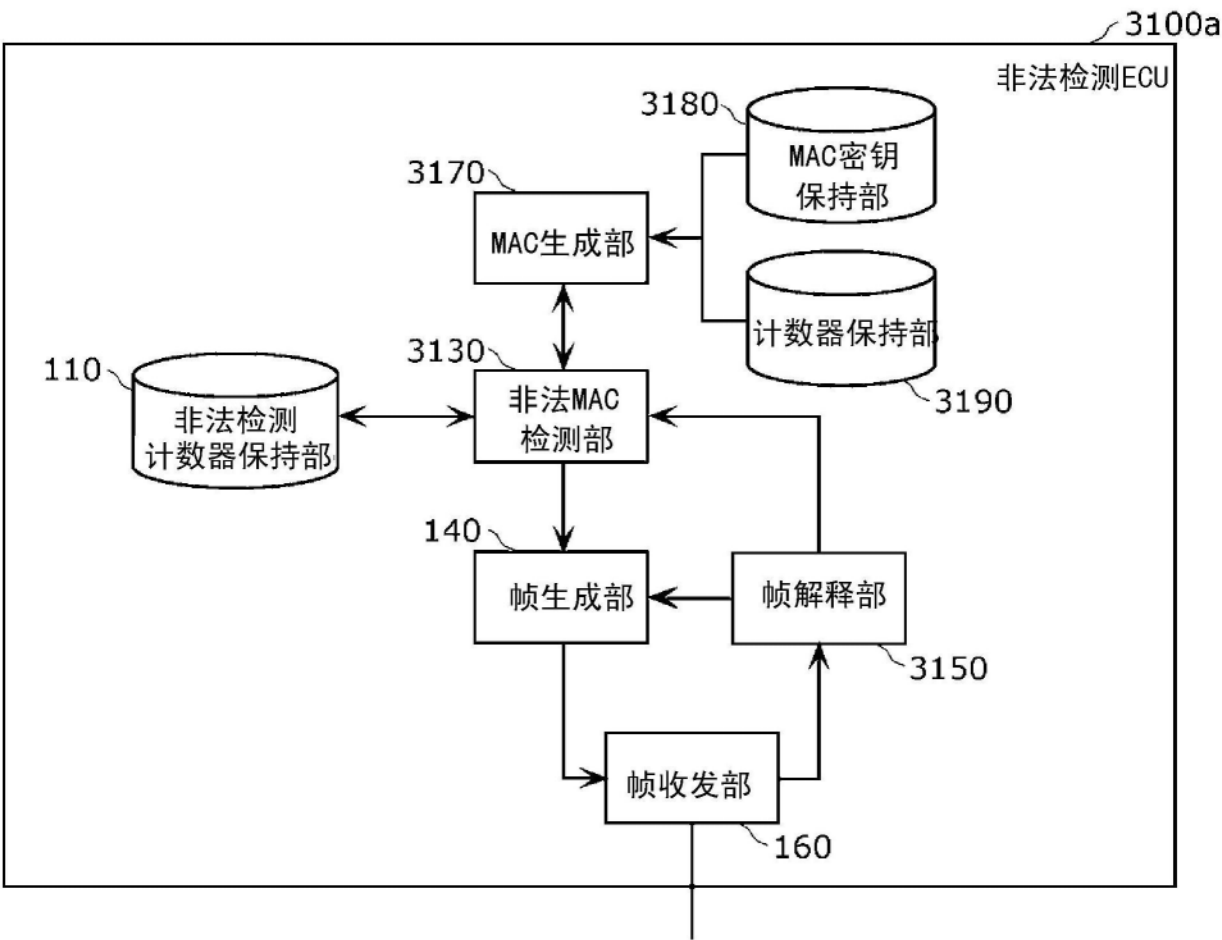


图30

ID	计数器
1	1
2	10
3	15
4	100
5	0
...	...

图31

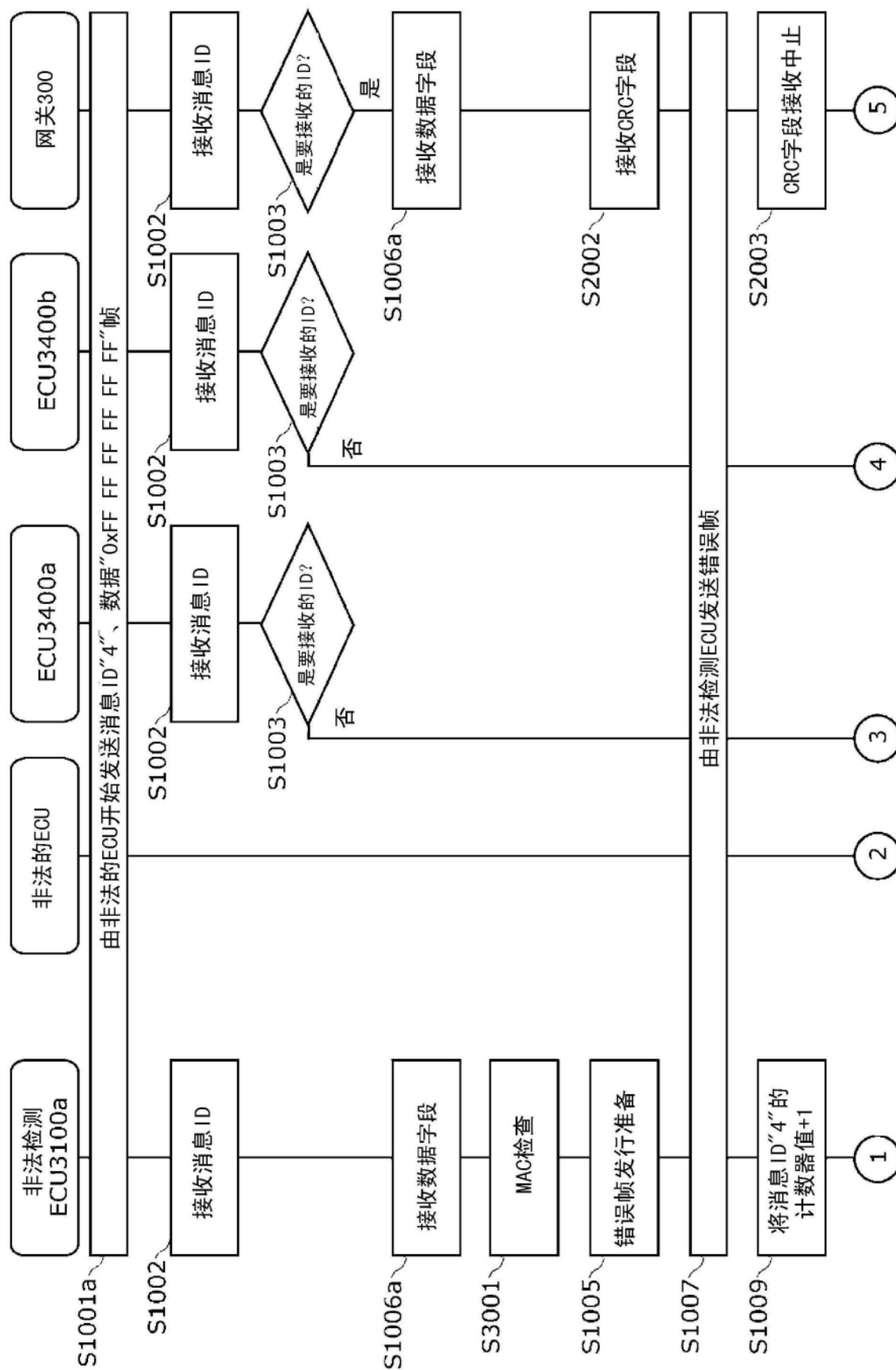


图32

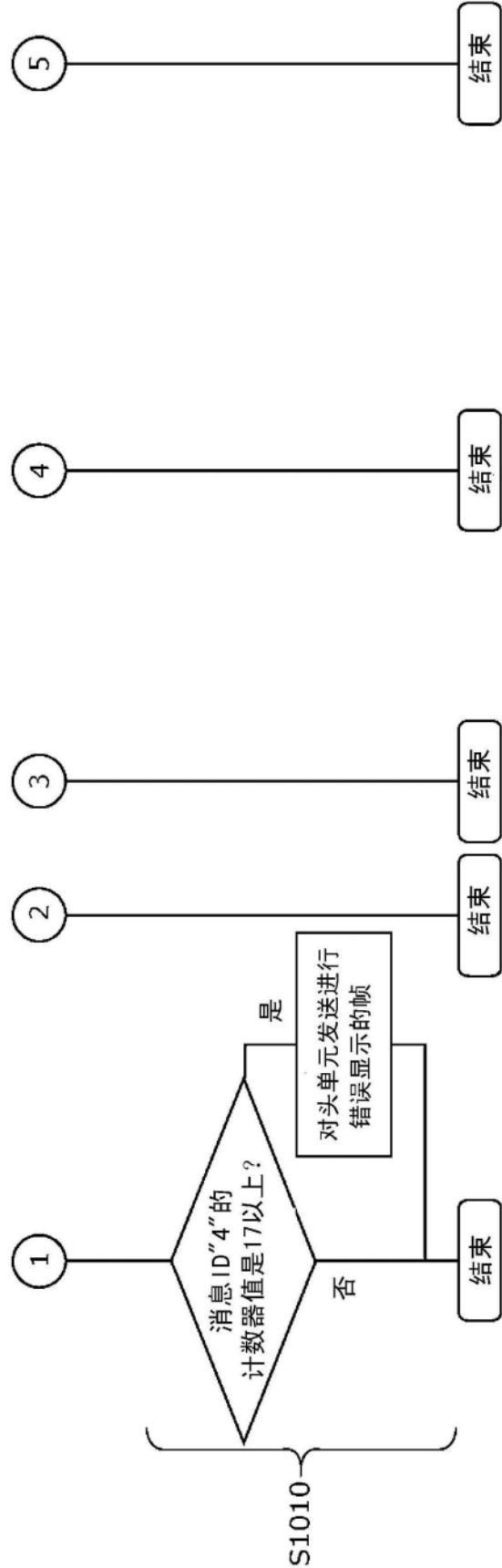


图33

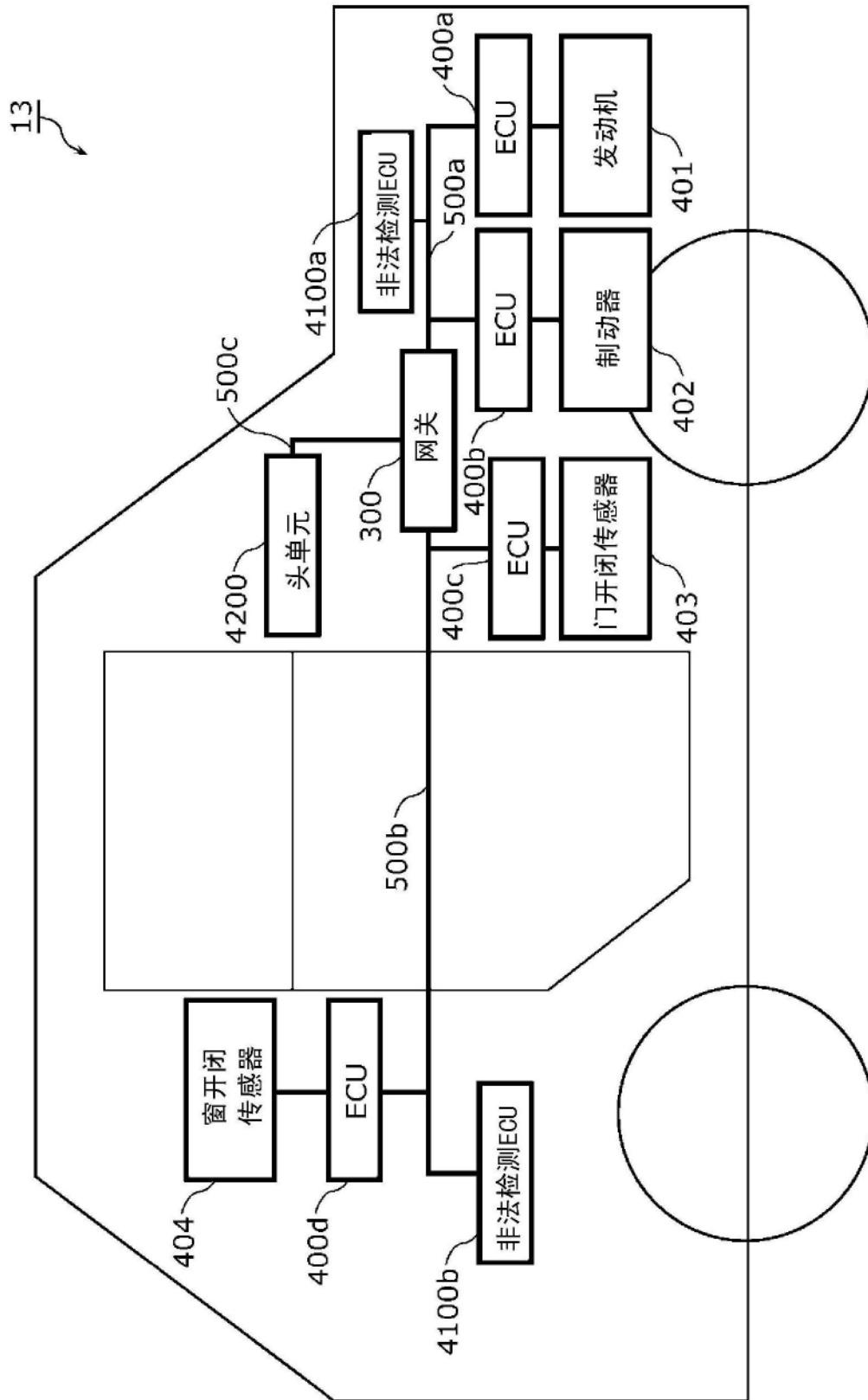


图34

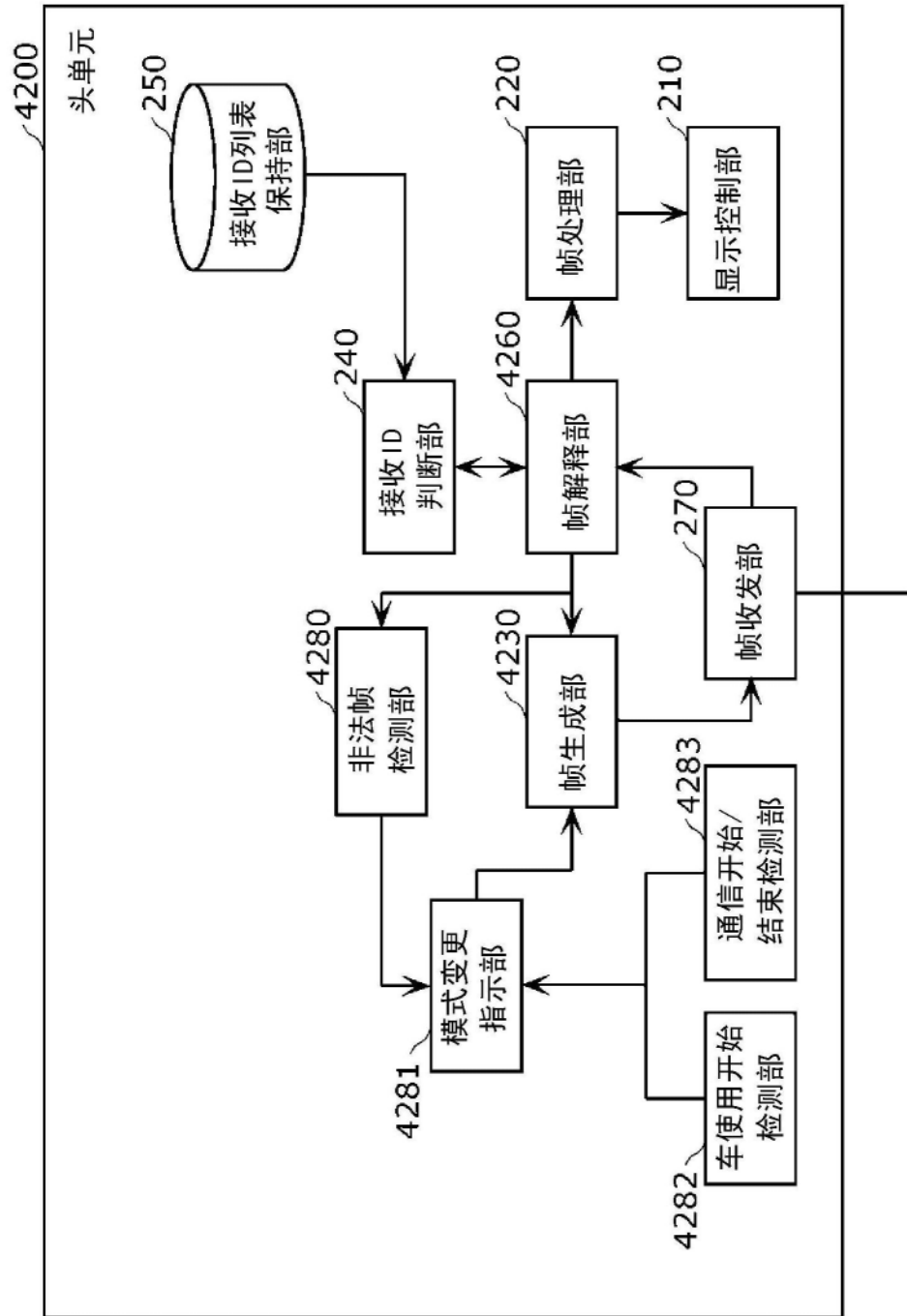


图35

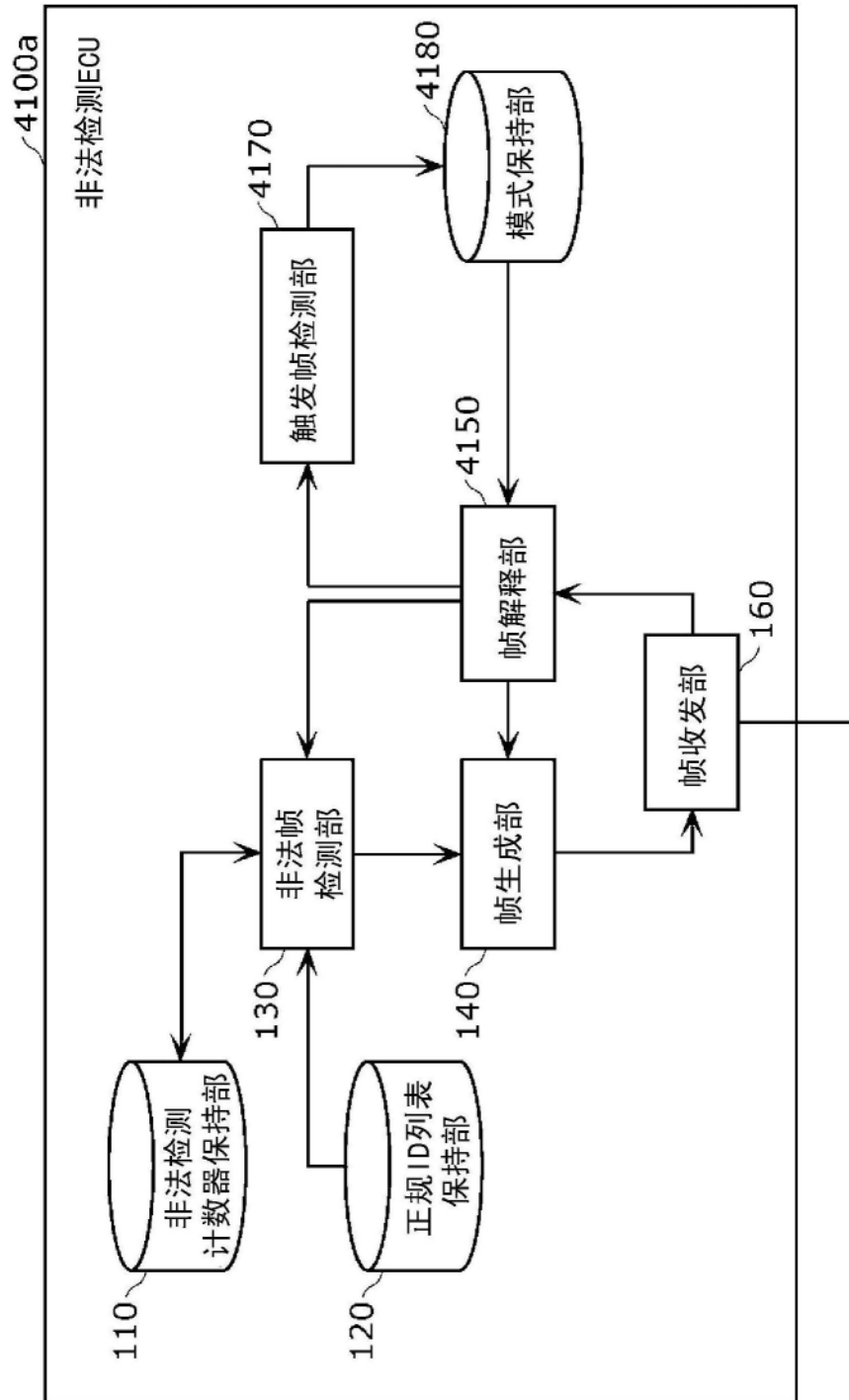


图36

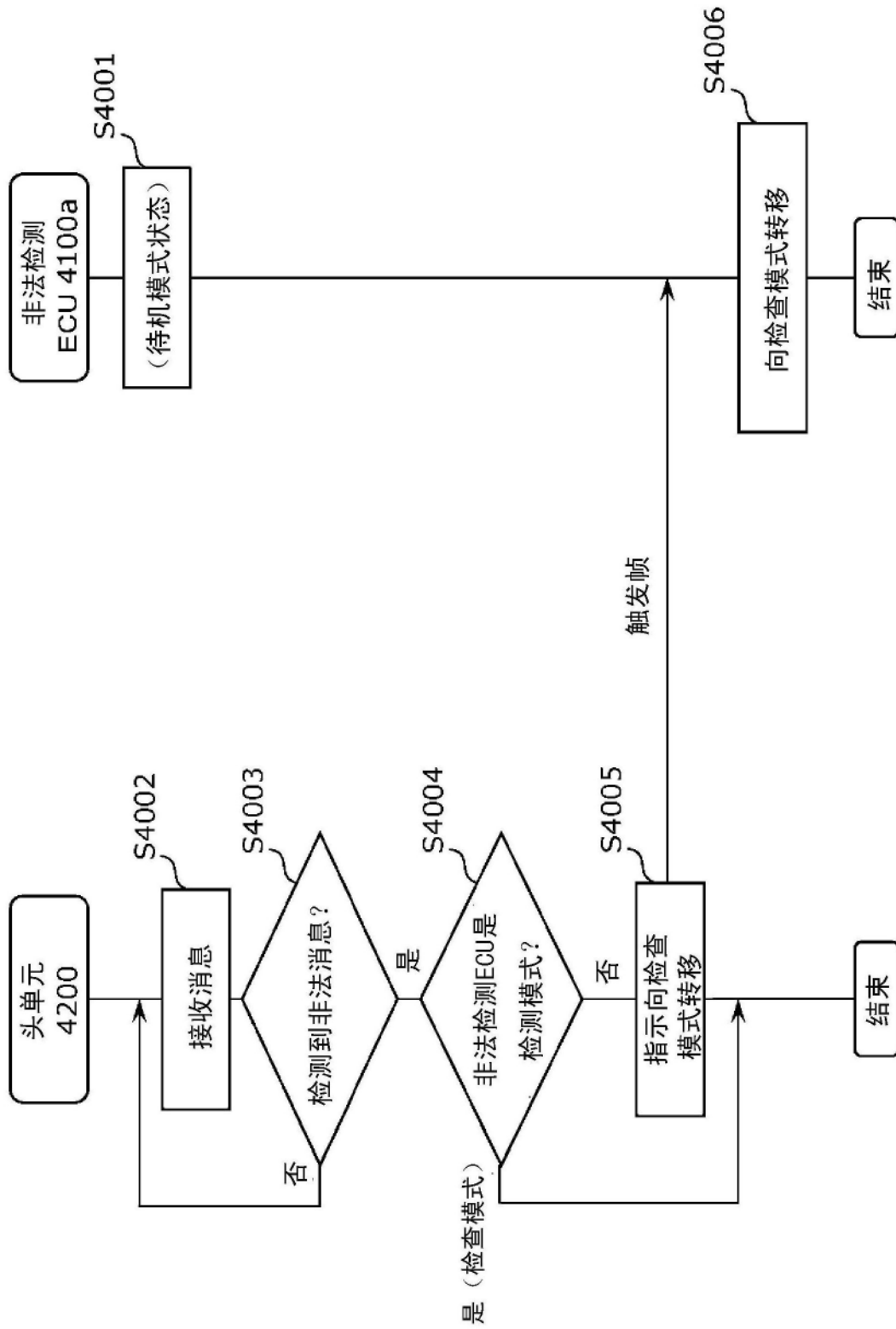


图37

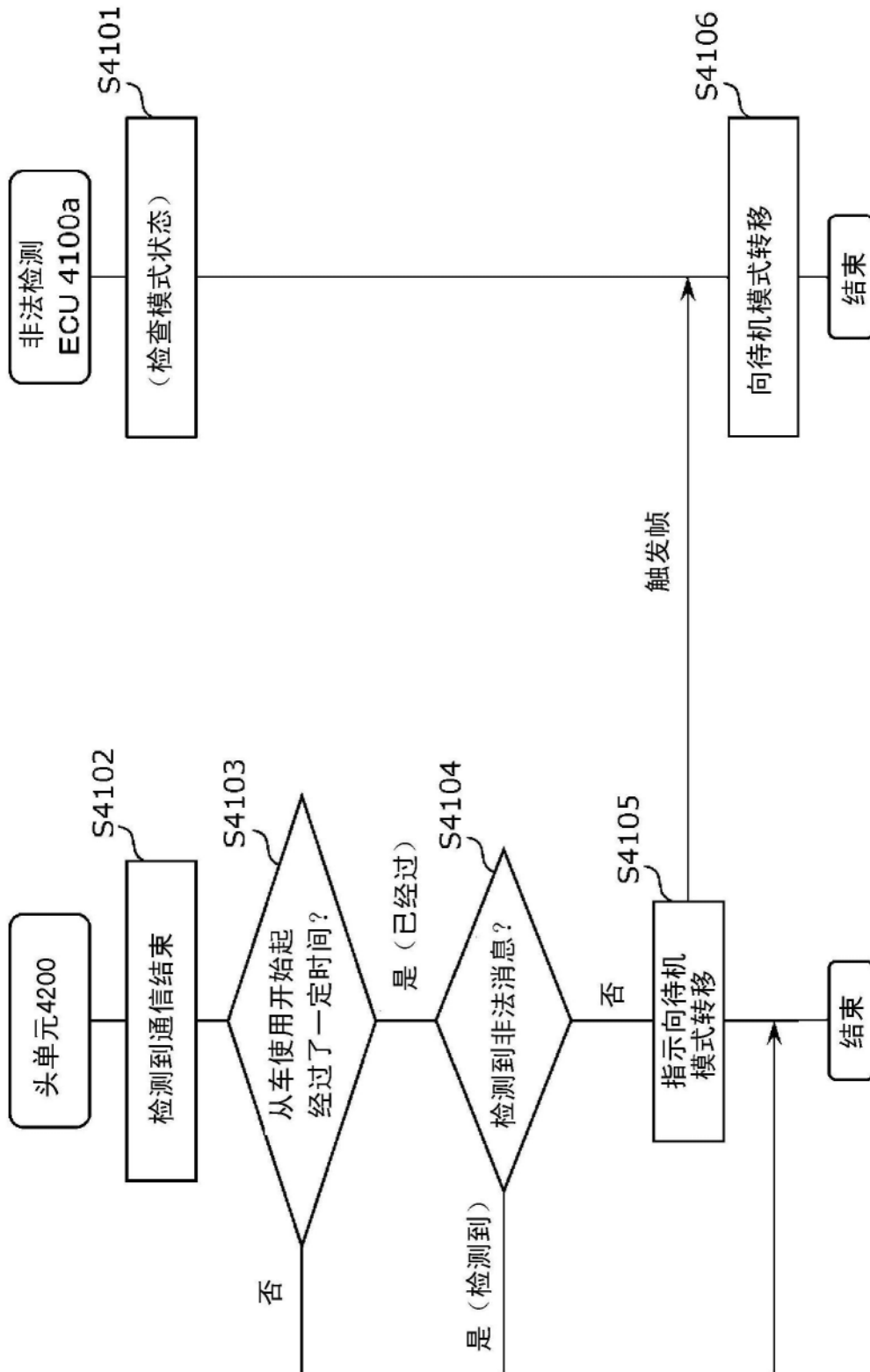


图38

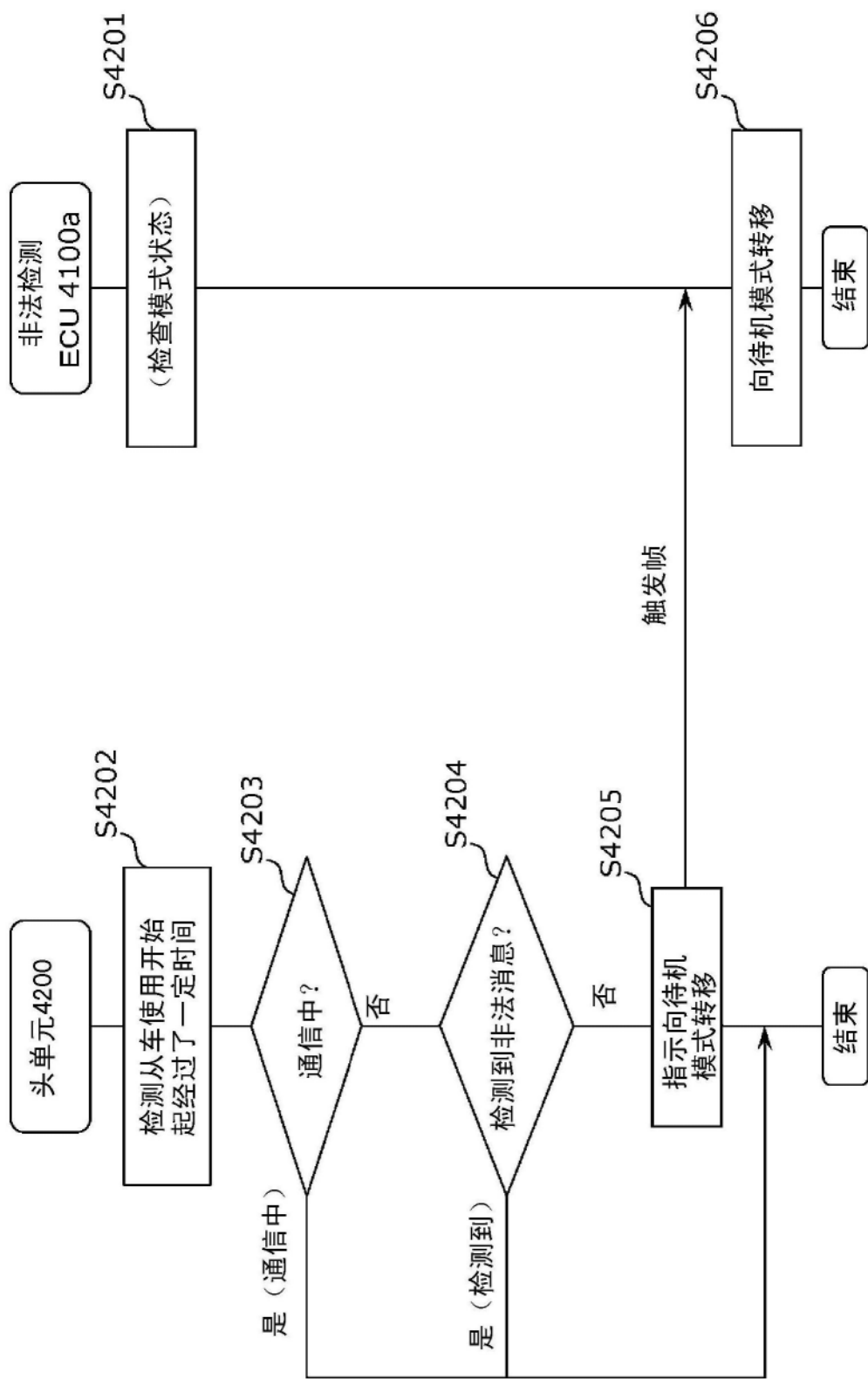


图39

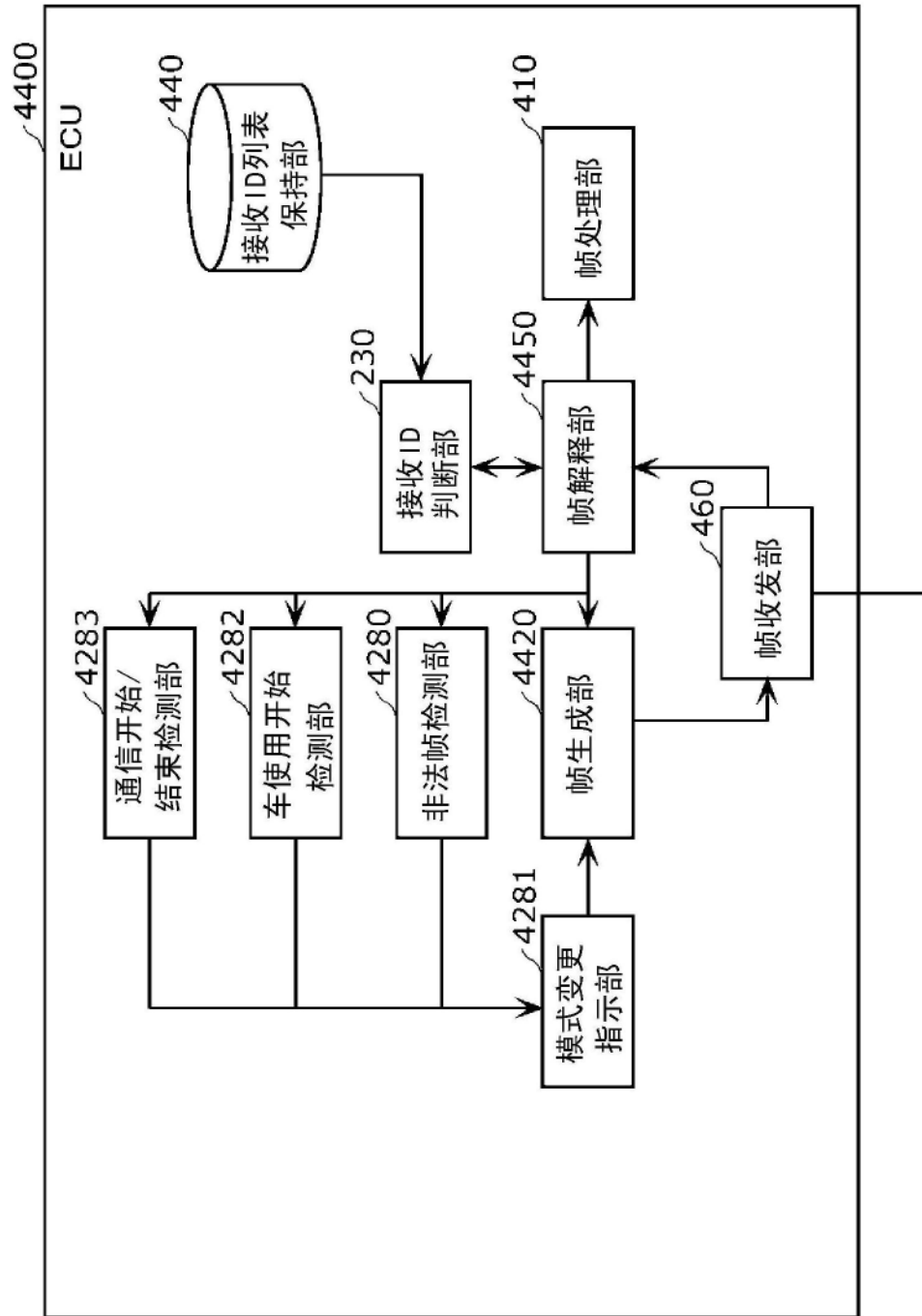


图40

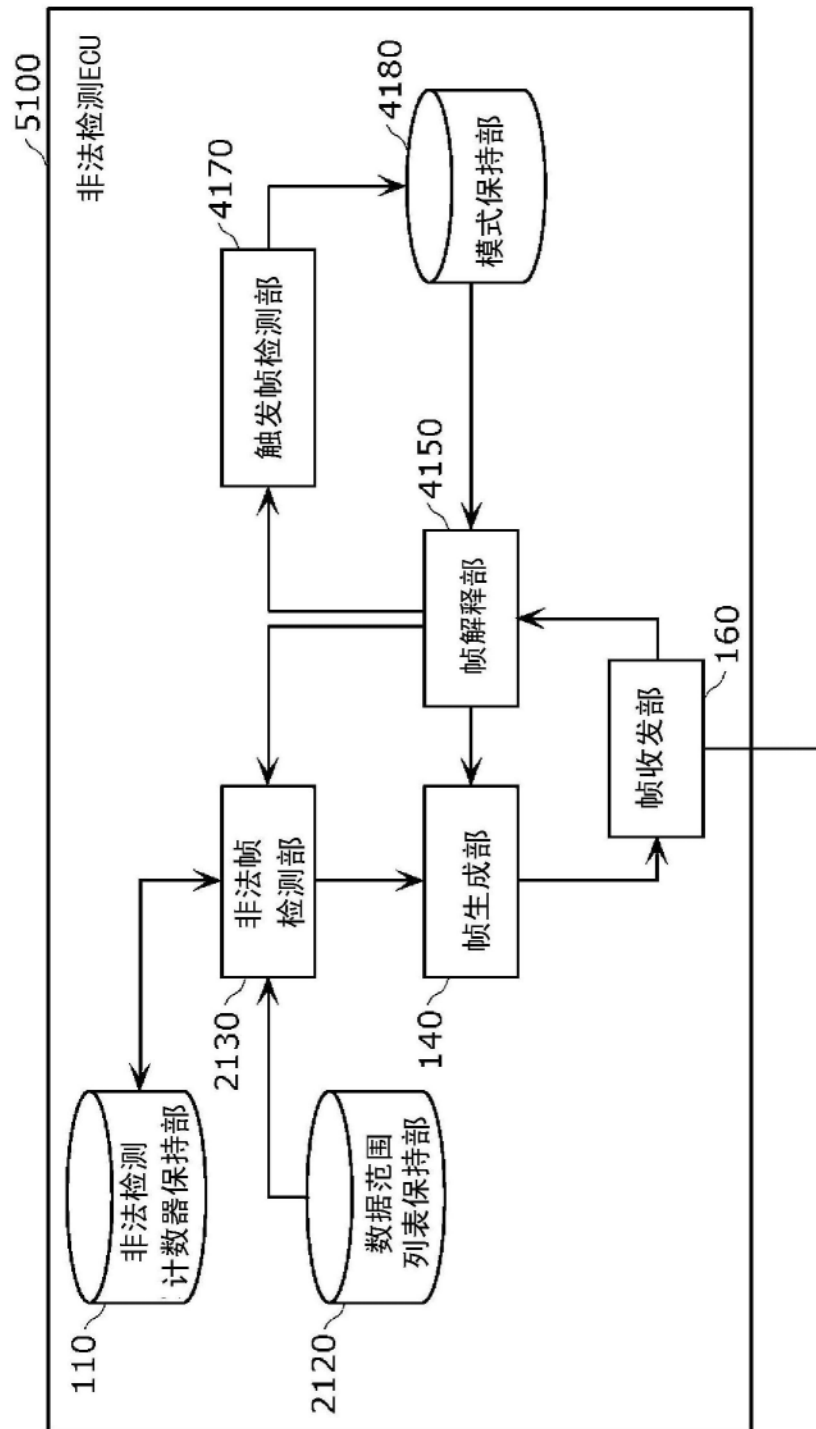


图41

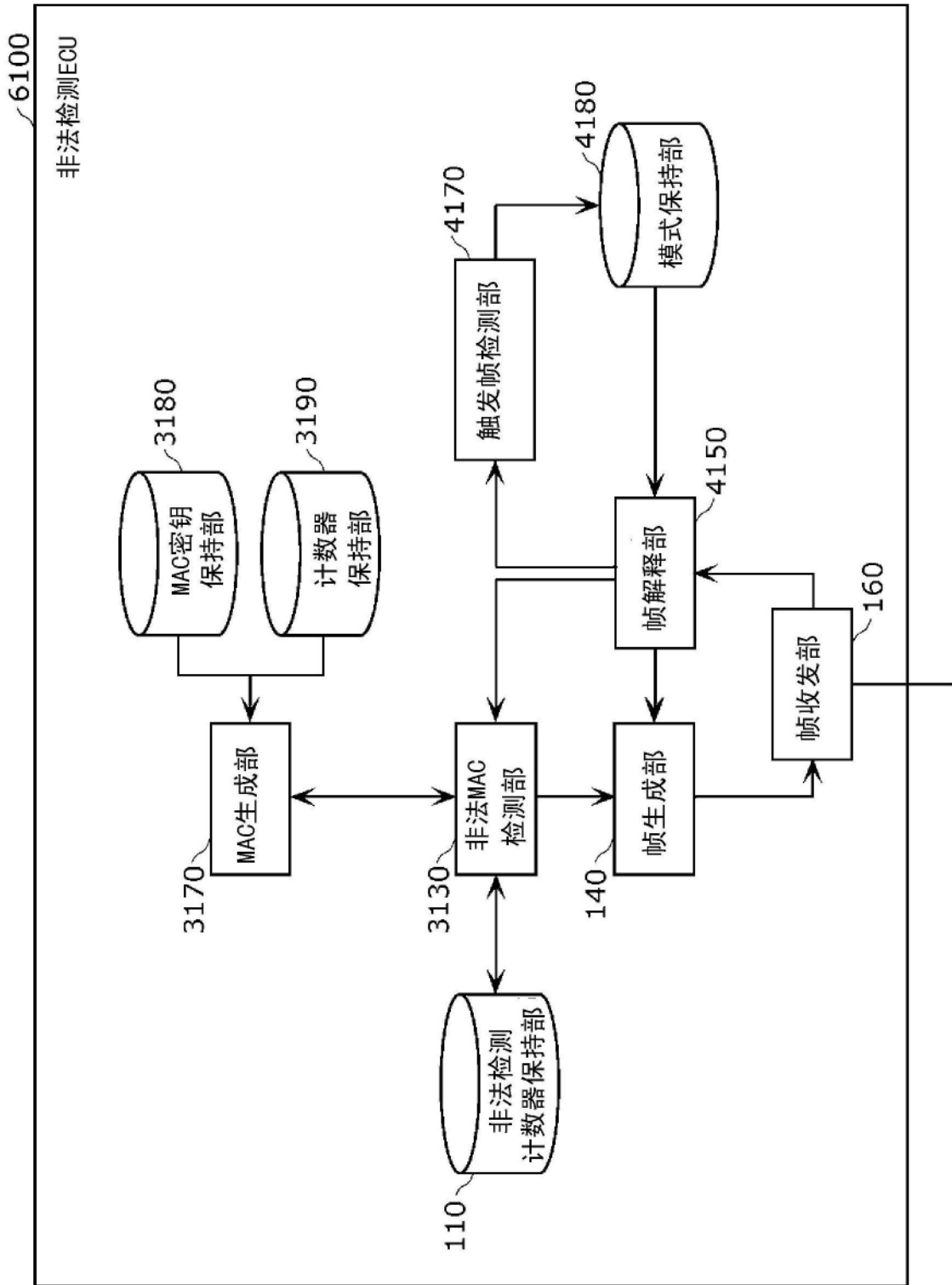


图42