

1. 一种不正常应对方法,是在具备多个电子控制单元的网络通信系统中使用的方法,所述多个电子控制单元利用网络进行通信,所述不正常应对方法包括:

第1判定步骤,通过所述多个电子控制单元中的一个电子控制单元判定已开始发送的帧中的预定域的内容是否符合表示不正常的预定条件;

发送步骤,在所述第1判定步骤中判定为所述帧的预定域的内容符合所述预定条件的情况下,通过所述一个电子控制单元在该帧的最末尾被发送之前发送错误帧;

记录步骤,通过所述一个电子控制单元按成为发送所述错误帧的对象的所述帧包含的ID域的内容所表示的各ID,对在所述发送步骤中发送了错误帧的次数进行记录;和

第2判定步骤,在通过所述记录步骤记录各ID的次数超过了预定次数的情况下判定为不正常,

所述预定次数表示与网络中的发送错误计数器的处理规则对应地确定的应该转变为消极状态的值,

在所述第2判定步骤中,在通过所述记录步骤记录各ID的次数超过所述预定次数的情况下,判定为发送了超过所述预定次数的所述ID的帧的电子控制单元为未转变为消极状态的不正常的电子控制单元。

2. 根据权利要求1所述的不正常应对方法,

在所述发送步骤中,在所述帧中的CRC序列的最末尾被发送之前,进行所述错误帧的所述发送。

3. 根据权利要求1所述的不正常应对方法,

所述预定域是表示ID的域,

在所述第1判定步骤中,通过将由所述预定域的内容表示的ID与预先确定的ID列表信息所表示的一个以上的ID进行比较,进行是否符合所述预定条件的所述判定。

4. 根据权利要求3所述的不正常应对方法,

在所述第1判定步骤中,在将由所述预定域的内容表示的ID与所述ID列表信息所表示的一个以上的全部ID全部进行比较而不一致的情况下,判定为符合所述预定条件。

5. 根据权利要求1所述的不正常应对方法,

所述预定域是控制域,

在所述第1判定步骤中,通过判别由所述预定域的内容表示的数据长度是否包含于预先确定的范围内,进行所述内容是否符合所述预定条件的所述判定。

6. 根据权利要求1所述的不正常应对方法,

在所述第1判定步骤中,在被发送的所述帧是数据帧的情况下进行所述判定,

所述预定域是数据域。

7. 根据权利要求6所述的不正常应对方法,

在所述第1判定步骤中,通过判别作为所述预定域的内容的数据值是否包含于预先确定的范围内,进行所述内容是否符合所述预定条件的所述判定。

8. 根据权利要求6所述的不正常应对方法,

在所述第1判定步骤中,通过预先确定的验证处理步骤对所述预定域的内容中的消息认证码进行验证,在该验证失败了的情况下,判定为所述内容符合所述预定条件。

9. 根据权利要求8所述的不正常应对方法,

由正常的电子控制单元发送的数据帧,在数据域内包含根据每次发送数据帧而变化的变量来推算的消息认证码,

在所述第1判定步骤中,在所述预定域的内容中的所述消息认证码未反映每次发送数据帧而变化的所述变量的情况下,判定为所述内容符合所述预定条件。

10.根据权利要求8所述的不正常应对方法,

由具有消息认证码密钥的正常的电子控制单元发送的数据帧,在数据域内包含使用所述消息认证码密钥生成的消息认证码,

在所述第1判定步骤中,使用与所述消息认证码密钥相呼应的密钥来进行所述预定域的内容中的所述消息认证码的所述验证。

11.一种不正常检测电子控制单元,其与多个电子控制单元在通信中所使用的网络连接,所述不正常检测电子控制单元具备:

接收部,其接收已开始发送的帧;

第1判定部,其判定由所述接收部接收到的帧中的预定域的内容是否符合表示不正常的预定条件;

发送部,其在所述第1判定部中判定为所述帧的预定域的内容符合所述预定条件的情况下,在该帧的最末尾被发送之前发送错误帧;

记录部,其按成为发送所述错误帧的对象的所述帧包含的ID域的内容所表示的各ID,对在所述发送部发送了错误帧的次数进行记录;以及

第2判定部,其在通过所述记录部记录的各ID的次数超过了预定次数的情况下判定为不正常,

所述预定次数表示与网络中的发送错误计数器的处理规则对应地确定的应该转变为消极状态的值,

在所述第2判定部中,在通过所述记录部记录的各ID的次数超过所述预定次数的情况下,判定为发送了超过所述预定次数的所述ID的帧的电子控制单元为未转变为消极状态的不正常的电子控制单元。

12.一种网络通信系统,具备多个电子控制单元和经由网络连接的不正常检测电子控制单元,

所述不正常检测电子控制单元具备:

接收部,其接收已开始发送的帧;

第1判定部,其判定由所述接收部接收到的帧中的预定域的内容是否符合表示不正常的预定条件;

发送部,其在所述第1判定部中判定为所述帧的预定域的内容符合所述预定条件的情况下,在该帧的最末尾被发送之前发送错误帧;

记录部,其按成为发送所述错误帧的对象的所述帧包含的ID域的内容所表示的各ID,对在所述发送部发送了错误帧的次数进行记录;以及

第2判定部,其在通过所述记录部记录的各ID的次数超过了预定次数的情况下判定为不正常,

所述预定次数表示与网络中的发送错误计数器的处理规则对应地确定的应该转变为消极状态的值,

在所述第2判定部中,在通过所述记录部记录的各ID的次数超过所述预定次数的情况下,判定为发送了超过所述预定次数的所述ID的帧的电子控制单元为未转变为消极状态的不正常的电子控制单元。

13.根据权利要求12所述的网络通信系统,

所述网络通信系统在所述多个电子控制单元的通信中使用多个网络,具备具有在所述多个网络之间传送帧的功能的网关装置、和分别与不同的网络连接的多个所述不正常检测电子控制单元,

所述预定域是表示ID的域,

所述第1判定部通过将由所述预定域的内容表示的ID与预先确定的ID列表信息表示的一个以上的ID进行比较,进行是否符合所述预定条件的所述判定,

所述ID列表信息按多个所述不正常检测电子控制单元的每一个而不同。

网络通信系统、不正常检测电子控制单元以及不正常应对方法

[0001] 本申请是申请日为2015年3月12日、申请号为201580012734.4、发明名称为“网络通信系统、不正常检测电子控制单元以及不正常应对方法”的中国专利申请的分案申请。

技术领域

[0002] 本公开涉及检测在电子控制单元进行通信的车载网络等中发送的不正常(fraud, 非法)帧并进行应对的技术。

背景技术

[0003] 近年来,在汽车中的系统内,配置有许多称为电子控制单元(ECU:Electronic Control Unit)的装置。连接这些ECU的网络称为车载网络。车载网络存在多种标准。作为其中最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(参照“非专利文献1”)。

[0004] 在CAN中,通信路径由两条总线构成,与总线连接的ECU称为节点。与总线连接的各节点收发被称为帧的消息。发送帧的发送节点通过在两条总线上施加电压,并在总线间产生电位差,从而发送被称为隐性(recessive)的值“1”和被称为显性(dominant)的值“0”。多个发送节点在完全相同的定时发送了隐性和显性的情况下,优先发送显性。接收节点在接收到的帧的格式存在异常的情况下,发送被称为错误帧(error frame)的帧。错误帧是通过连续地发送6比特(bit)的显性,从而向发送节点和/或其他接收节点通知帧的异常的帧。

[0005] 另外,在CAN中不存在指示发送目的地或发送源的识别符,发送节点在每帧中附加被称为消息ID的ID并进行发送(也即是,向总线送出信号),各接收节点仅接收预先确定的消息ID(也即是,从总线读取信号)。另外,采用CSMA/CA(Carrier Sense Multiple Access/Collision Avoidance:载波侦听多址访问/冲突避免)方式,在多个节点的同时发送时,进行利用消息ID的仲裁(调停),优先发送消息ID的值小的帧。

[0006] 现有技术文献

[0007] 非专利文献

[0008] 非专利文献1:CAN Specification 2.0part A,[online],CAN in Automation (CiA),[2014年11月14日检索],互联网(URL:<http://www.can-cia.org/fileadmin/cia/specifications/CAN20A.pdf>)

[0009] 非专利文献2:RFC2104 HMAC:Keyed-Hashing for Message Authentication

发明内容

[0010] 发明要解决的技术问题

[0011] 然而,在车载网络中,存在因不正常节点连接到总线且不正常节点不正常地发送帧,从而导致不正常地控制车体的可能性。

[0012] 因此,本公开提供一种在车载网络等遵循CAN协议进行通信的网络通信系统中阻

止由ECU执行基于发送到总线的不正常帧的处理的ECU(不正常检测ECU)。另外,本公开提供一种阻止与不正常帧对应的处理被执行的不正常应对方法以及具备不正常检测ECU的网络通信系统。

[0013] 用于解决问题的技术方案

[0014] 为了解决上述问题,本公开的一个技术方案涉及的不正常应对方法是在具备多个电子控制单元的网络通信系统中使用的方法,所述多个电子控制单元遵循CAN协议即控制器局域网协议经由总线进行通信,所述不正常应对方法包括:判定步骤,判定已开始发送的帧中的预定域的内容是否符合表示不正常的预定条件;和发送步骤,在所述判定步骤中判定为所述帧的预定域的内容符合所述预定条件的情况下,在该帧的最末尾被发送之前发送错误帧。

[0015] 另外,为了解决上述问题,本公开的一个技术方案涉及的不正常检测电子控制单元是与遵循CAN协议即控制器局域网协议进行通信的多个电子控制单元在通信中所使用的总线连接的单元,所述不正常检测电子控制单元具备:接收部,其接收已开始发送的帧;判定部,其判定由所述接收部接收到的帧中的预定域的内容是否符合表示不正常的预定条件;以及发送部,其在所述判定部中判定为所述帧的预定域的内容符合所述预定条件的情况下,在该帧的最末尾被发送之前发送错误帧。

[0016] 另外,为了解决上述问题,本公开的一个技术方案涉及的网络通信系统具备遵循CAN协议即控制器局域网协议经由总线进行通信的多个电子控制单元和与该总线连接的不正常检测电子控制单元,所述不正常检测电子控制单元具备:接收部,其接收已开始发送的帧;判定部,其判定由所述接收部接收到的帧中的预定域的内容是否符合表示不正常的预定条件;以及发送部,其在所述判定部中判定为所述帧的预定域的内容符合所述预定条件的情况下,在该帧的最末尾被发送之前发送错误帧。

[0017] 发明的效果

[0018] 根据本公开,在遵循CAN协议进行通信的网络通信系统中,即使不正常节点连接到总线并发送了不正常帧,也能够阻止由ECU执行基于不正常帧的处理。

附图说明

[0019] 图1是表示实施方式1涉及的车载网络系统的整体构成的图。

[0020] 图2是表示由CAN协议规定的帧的格式的图。

[0021] 图3是表示由CAN协议规定的错误帧的格式的图。

[0022] 图4是头单元的构成图。

[0023] 图5是示出了接收ID列表的一例的图。

[0024] 图6是网关的构成图。

[0025] 图7是示出了传送规则的一例的图。

[0026] 图8是实施方式1涉及的ECU的构成图。

[0027] 图9是示出了接收ID列表的一例的图。

[0028] 图10是表示从与发动机连接的ECU发送的帧的ID以及数据域的一例的图。

[0029] 图11是表示从与制动器连接的ECU发送的帧的ID以及数据域的一例的图。

[0030] 图12是表示从与门开闭传感器连接的ECU发送的帧的ID以及数据域的一例的图。

- [0031] 图13是表示从与窗开闭传感器连接的ECU发送的帧的ID以及数据域的一例的图。
- [0032] 图14是实施方式1涉及的不正常检测ECU的构成图。
- [0033] 图15是示出了不正常检测ECU所保持的正规ID列表的一例的图。
- [0034] 图16是示出了不正常检测ECU所保持的正规ID列表的一例的图。
- [0035] 图17是表示各个消息ID的不正常检测计数器的状态的一例的图。
- [0036] 图18是表示实施方式1中的与不正常帧的检测以及执行阻止相关的工作例的时序图。
- [0037] 图19是表示实施方式2涉及的车载网络系统的整体构成的图。
- [0038] 图20是实施方式2涉及的不正常检测ECU的构成图。
- [0039] 图21是示出了不正常检测ECU所保持的数据范围列表的一例的图。
- [0040] 图22是表示实施方式2中的与不正常帧的检测以及执行阻止相关的工作例的时序图(后接图23)。
- [0041] 图23是表示实施方式2中的与不正常帧的检测以及执行阻止相关的工作例的时序图(前接图22)。
- [0042] 图24是表示实施方式3涉及的车载网络系统的整体构成的图。
- [0043] 图25是实施方式3涉及的ECU的构成图。
- [0044] 图26是表示从与发动机连接的ECU发送的数据帧的ID以及数据域的一例的图。
- [0045] 图27是表示从与制动器连接的ECU发送的数据帧的ID以及数据域的一例的图。
- [0046] 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以及数据域的一例的图。
- [0047] 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以及数据域的一例的图。
- [0048] 图30是实施方式3涉及的不正常检测ECU的构成图。
- [0049] 图31是表示实施方式3涉及的计数器保持部所保持的各个消息ID的计数器值的一例的图。
- [0050] 图32是表示实施方式3中的与不正常帧的检测以及执行阻止相关的工作例的时序图(后接图33)。
- [0051] 图33是表示实施方式3中的与不正常帧的检测以及执行阻止相关的工作例的时序图(前接图32)。

具体实施方式

[0052] 本公开的一个技术方案涉及的不正常应对方法是在具备多个电子控制单元的网络通信系统中使用的方法,所述多个电子控制单元遵循CAN协议即控制器局域网协议经由总线进行通信,所述不正常应对方法包括:判定步骤,判定已开始发送的帧中的预定域的内容是否符合表示不正常的预定条件;和发送步骤,在所述判定步骤中判定为所述帧的预定域的内容符合所述预定条件的情况下,在该帧的最末尾被发送之前发送错误帧。此外,作为表示不正常的预定条件的一例,可例如列举如下等条件:预定域的内容未包含在表示正常(正当)值组的列表中;预定域的内容包含在表示不正常值组的列表中;预定域的内容处于一定范围内或者为具有一定特征的值(例如偶数等);对内容值实施了预定运算得到的结果

成为预定值。由此,在遵循CAN协议进行通信的网络通信系统中,即使不正常节点连接到总线并发送了不正常帧,也能够阻止由各节点(ECU)执行基于不正常帧的处理。

[0053] 另外,也可以为,在所述发送步骤中,在所述帧中的CRC序列的最末尾被发送之前,进行所述错误帧的所述发送。由此,例如,能够使得确认CRC序列并处理帧的ECU不执行基于不正常帧的处理。

[0054] 另外,也可以为,所述预定域是表示ID的域,在所述判定步骤中,通过将由所述预定域的内容表示的ID与预先确定的ID列表信息所表示的一个以上的ID进行比较,进行是否符合所述预定条件的所述判定。由此,例如,能够通过数据帧或远程帧中的ID域来判断是否不正常,能够阻止各ECU执行关于不正常帧的处理。

[0055] 另外,也可以为,所述预定域是控制域,在所述判定步骤中,通过判别由所述预定域的内容表示的数据长度是否包含于预先确定的范围内,进行所述内容是否符合所述预定条件的所述判定。由此,例如,能够通过数据帧或远程帧中的控制域来判断是否不正常,能够阻止各ECU执行关于不正常帧的处理。

[0056] 另外,也可以为,在所述判定步骤中,在被发送的所述帧是数据帧的情况下进行所述判定,所述预定域是数据域。由此,能够阻止各ECU按照不正常的数据帧的数据来执行与该数据对应的处理。

[0057] 另外,也可以为,在所述判定步骤中,通过判别作为所述预定域的内容的数据值是否包含于预先确定的范围内,进行所述内容是否符合所述预定条件的所述判定。由此,例如即使发送了包含不正常范围的数据值的不正常的数据帧,也能够阻止各ECU执行与该数据对应的处理。

[0058] 另外,也可以为,在所述判定步骤中,通过预先确定的验证处理步骤对所述预定域的内容中的消息认证码进行验证,在该验证失败了的情况下,判定为所述内容符合所述预定条件。由此,在发送了未附加正规的消息认证码的不正常帧的情况下,能够阻止各ECU执行关于不正常帧的处理。

[0059] 另外,也可以为,由正常(正当)的电子控制单元发送的数据帧,在数据域内包含根据每次发送数据帧而变化的变量来推算的消息认证码,在所述判定步骤中,在所述预定域的内容中的所述消息认证码未反映每次发送数据帧而变化的所述变量的情况下,判定为所述内容符合所述预定条件。由此,例如能够使得难以进行对于消息认证码的不正常解读。

[0060] 另外,也可以为,由具有消息认证码密钥的正常(正当)的电子控制单元发送的数据帧,在数据域内包含使用所述消息认证码密钥生成的消息认证码,在所述判定步骤中,使用与所述消息认证码密钥相呼应的密钥来进行所述预定域的内容中的所述消息认证码的所述验证。由此,例如关于正规的多个ECU,能够共用除消息认证码密钥之外的用于消息认证码生成的结构。

[0061] 另外,也可以为,所述不正常应对方法还包括:记录步骤,对在所述发送步骤中发送了错误帧的次数进行记录;和报告步骤,在通过所述记录步骤记录的次数超过了预定次数的情况下进行报告。由此,能够在反复发送了不正常帧的情况下向用户等进行报告。

[0062] 另外,本公开的一个技术方案涉及的不正常检测电子控制单元(不正常检测ECU)是与遵循CAN协议即控制器局域网协议进行通信的多个电子控制单元在通信中所使用的总线连接的单元,所述不正常检测电子控制单元具备:接收部,其接收已开始发送的帧;判定

部,其判定由所述接收部接收到的帧中的预定域的内容是否符合表示不正常的预定条件;以及发送部,其在所述判定部中判定为所述帧的预定域的内容符合所述预定条件的情况下,在该帧的最末尾被发送之前发送错误帧。由此,在遵循CAN协议进行通信的网络通信系统中,即使不正常节点连接到对遵循CAN协议进行通信的多个ECU进行连接的总线并发送了不正常帧,也能够阻止由各ECU执行基于不正常帧的处理。

[0063] 另外,本公开的一个技术方案涉及的网络通信系统具备遵循CAN协议即控制器局域网协议经由总线进行通信的多个电子控制单元和与该总线连接的不正常检测电子控制单元,所述不正常检测电子控制单元具备:接收部,其接收已开始发送的帧;判定部,其判定由所述接收部接收到的帧中的预定域的内容是否符合表示不正常的预定条件;以及发送部,其在所述判定部中判定为所述帧的预定域的内容符合所述预定条件的情况下,在该帧的最末尾被发送之前发送错误帧。由此,即使不正常节点连接到总线并发送了不正常帧,也能够阻止由ECU执行基于不正常帧的处理。

[0064] 此外,这些总括性或具体的技术方案既可以通过系统、方法、集成电路、计算机程序或者计算机可读的CD-ROM等记录介质来实现,也可以通过系统、方法、集成电路、计算机程序和记录介质的任意组合来实现。

[0065] 以下,参照附图对实施方式涉及的不正常检测ECU进行说明。在此所示的实施方式均表示本公开的一个具体例子。因此,以下的实施方式中示出的数值、构成要素、构成要素的配置以及连接方式、步骤(工序)以及步骤的顺序等是一个例子,并不是限定本公开。关于以下的实施方式中的构成要素中的未记载在独立权利要求中的构成要素,是能够任意附加的构成要素。另外,各图是示意图,不一定是严格图示。

[0066] (实施方式1)

[0067] 以下,作为本公开的实施方式,使用附图对包含不正常检测ECU的车载网络系统10进行说明,所述不正常检测ECU实现用于使用消息ID来阻止在其他节点(ECU)中执行基于不正常帧的处理的不正常应对方法。

[0068] [1.1 车载网络系统10的整体构成]

[0069] 图1是表示实施方式1涉及的车载网络系统10的整体构成的图。车载网络系统10是遵循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中的网络通信系统。车载网络系统10构成为包括:总线500a、500b、不正常检测ECU100a、100b、头单元200、网关300、以及与各种设备连接的ECU400a~400d等ECU这种连接于总线的各节点。此外,尽管在图1中进行了省略,但车载网络系统10除了ECU400a~400d以外还可以包括很多ECU,但在此为了方便而着眼于ECU400a~400d来进行说明。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、通信线路等的装置。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)。例如通过处理器按照控制程序(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的功能而组合多个表示对处理器的指令的命令代码而构成的。在此,以有可能会在总线500a、500b上连接有发送不正常帧的不正常ECU为前提来进行说明。

[0070] 不正常检测ECU100a、100b分别连接于总线500a、总线500b,是具有如下功能的ECU:判定由ECU400a~400d等发送的帧是否不正常,如果不正常则发送错误帧。

[0071] ECU400a~400d与任一条总线连接,另外,ECU400a~400d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。

[0072] 网关300与连接不正常检测ECU100a、ECU400a以及ECU400b的总线500a、连接不正常检测ECU100b、ECU400c以及ECU400d的总线500b、和连接头单元200的总线500c连接,具有将从各条总线接收到的帧传送给其他总线的功能。另外,也能够按所连接的各总线间来切换是否传送所接收到的帧。网关300也是一种ECU。

[0073] 头单元200具有接收帧的功能,具有如下功能:接收从ECU400a~400d发送的帧,将各种状态显示于显示器(未图示),并提示给用户。头单元200也是一种ECU。

[0074] 在该车载网络系统10中,各ECU遵循CAN协议进行帧的授受。CAN协议的帧有数据帧、远程帧、过载帧以及错误帧。为了便于说明,首先以数据帧以及错误帧为中心来说明。

[0075] [1.2数据帧格式]

[0076] 以下,对作为在遵循CAN协议的网络中使用的帧之一的数据帧进行说明。

[0077] 图2是表示由CAN协议规定的帧的格式的图。该图示出了由CAN协议规定的标准ID格式的数据帧。数据帧由SOF(Start Of Frame,帧起始)、ID域(field)、RTR(Remote Transmission Request,远程发送请求)、IDE(Identifier Extension,标识符扩展)、预约位“r”、DLC(Data Length Code,数据长度码)、数据域、CRC(Cyclic Redundancy Check,循环冗余校验)时序、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)的各域构成。

[0078] SOF由1比特的显性构成。总线空闲的状态成为隐性,通过由SOF变更为显性,通知帧的发送开始。

[0079] ID域是由11比特构成的保存表示数据种类的值即ID(消息ID)的域。在多个节点同时开始了发送的情况下,为了通过该ID域进行通信仲裁,设计成使具有ID小的值的帧具有高优先级。

[0080] RTR是用于识别数据帧和远程帧的值,在数据帧中由1比特的显性构成。

[0081] IDE和“r”两方都由1比特的显性构成。

[0082] DLC由4比特构成,是表示数据域的长度的值。此外,将IDE、“r”以及DLC一起称为控制域。

[0083] 数据域是最大64由比特构成的表示要发送的数据的内容的值。能够按每8比特来调整长度。所发送的数据的规格不在CAN协议中规定,而在车载网络系统10中确定。因此,为取决于车型、制造者(制造商)等的规格。

[0084] CRC序列由15比特构成。根据SOF、ID域、控制域以及数据域的发送值来算出。

[0085] CRC定界符是由1比特的隐性构成的表示CRC序列的结束的分隔符号。此外,将CRC序列和CRC定界符一起称为CRC域。

[0086] ACK间隙由1比特构成。发送节点将ACK间隙设为隐性并进行发送。如果到CRC序列为止能够正常接收,则接收节点将ACK间隙设为显性并发送。由于显性比隐性优先,因此,如果在发送后ACK间隙为显性,则发送节点能够确认某一个接收节点接收成功。

[0087] ACK定界符由1比特的隐性构成,是表示ACK的结束的分隔符号。

[0088] EOF由7比特的隐性构成,表示数据帧的结束。

[0089] [1.3错误帧格式]

[0090] 图3是表示由CAN协议规定的错误帧的格式的图。错误帧包括错误标志(初级)、错误标志(次级)和错误定界符。

[0091] 错误标志(初级)为了向其他节点通知错误的产生而使用。检测到错误的节点为了向其他节点通知错误的产生而连续发送6比特的显性。该发送违反CAN协议的位填充(bit stuffing)规则(不连续发送6比特以上的相同值),引起来自其他节点的错误帧(次级)的发送。

[0092] 错误标志(次级)由为了向其他节点通知错误的产生而使用的连续的6比特的显性构成。接收到错误标志(初级)而检测到违反了位填充规则的全部节点会发送错误标志(次级)。

[0093] 错误定界符“DEL”是8比特的连续的隐性,表示错误帧的结束。

[0094] [1.4头单元200的构成]

[0095] 头单元(head unit)200例如设置于汽车的仪表板等,是具备显示用于驾驶员视觉辨认的信息的液晶显示器(LCD:liquid crystal display)等显示装置、受理驾驶员的操作的输入单元等的一种ECU。

[0096] 图4是头单元200的构成图。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,该各功能通过头单元200中的通信线路、LCD、执行存储器所保存的控制程序的处理器或数字电路等实现。

[0097] 帧收发部270相对于总线500c收发遵循CAN协议的帧。从总线500c逐比特地接收帧,并传送给帧解释部260。另外,将从帧生成部230收到通知的帧的内容逐比特地发送到总线500c。

[0098] 帧解释部260从帧收发部270接收帧的值,并进行解释以使得向由CAN协议规定的帧格式的各领域进行映射。帧解释部260将判断为ID域的值传送给接收ID判断部240。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域的值和ID域之后出现的数据域传送给帧处理部220还是在收到该判定结果之后中止帧的接收(即中止作为该帧的解释)。另外,帧解释部260例如在CRC的值不符或设为显性固定的项目却为隐性等判断为是未遵循CAN协议的帧的情况下,向帧生成部230进行通知,以使得发送错误帧。另外,帧解释部260在接收到错误帧的情况下,即在根据所接收到的帧的值而解释为成为错误帧的情况下,自此之后丢弃该帧,即中止帧的解释。例如在从数据帧的中途起解释为错误帧的情况下,中止该数据帧的解释,不会再根据该数据帧来进行特别的处理。

[0099] 接收ID判断部240接收从帧解释部260通知的ID域的值,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域之后的帧的各域的判定。接收ID判断部240将该判定结果通知给帧解释部260。

[0100] 接收ID列表保持部250保持头单元200接收到的ID(消息ID)的列表即接收ID列表。图5是示出了接收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为“1”的帧(消息),从与制动器402连接的ECU400b接收消息ID为“2”的帧,从与门开闭传感器403连接的ECU400c接收消息ID为“3”的帧,从与窗开闭传感器404连接的ECU400d接收消息ID为“4”的帧。

[0101] 帧处理部220基于所接收到的帧的内容(例如消息ID以及数据域的内容),形成例

如应显示于LCD的图像,并通知给显示控制部210。此外,帧处理部220也可以保持所接收到的数据域的内容,根据经由输入单元受理的驾驶员的操作,选择应显示于LCD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)来进行通知。

[0102] 显示控制部210将从帧处理部220收到了通知的内容显示于LCD等。

[0103] 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,将错误帧通知给帧收发部270并使其发送该错误帧。

[0104] [1.5接收ID列表例1]

[0105] 上述的图5是表示在头单元200、网关300、ECU400c以及ECU400d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列表用于选择性地接收包含ID(消息ID)的值为“1”、“2”、“3”和“4”的某一个的消息ID的帧并进行处理。例如,若在头单元200的接收ID列表保持部250中保持有图5的接收ID列表,则关于消息ID不为“1”、“2”、“3”和“4”的任一个的帧,中止帧解释部260中的ID域以后的帧的解释。

[0106] [1.6网关300的构成]

[0107] 图6是网关300的构成图。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、传送处理部310和传送规则保持部370。这些各构成要素是功能性的构成要素,该各功能通过网关300中的通信线路、执行存储器所保存的控制程序的处理器或数字电路等来实现。

[0108] 帧收发部360相对于总线500a、500b、500c分别收发遵循CAN协议的帧。从总线逐比特地接收帧,并传送给帧解释部350。另外,基于从帧生成部320收到了通知的表示传送目的地的总线的总线信息以及帧,将该帧的内容逐比特地发送到总线500a、500b、500c。

[0109] 帧解释部350从帧收发部360接收帧的值,进行解释以使得向由CAN协议规定的帧格式的各领域进行映射。判断为ID域的值被传送给接收ID判断部330。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域的值和ID域之后出现的数据域(数据)传送给传送处理部310还是在收到该判定结果之后中止帧的接收(即中止作为该帧的解释)。另外,帧解释部350在判断为是未遵循CAN协议的帧的情况下,向帧生成部320进行通知,以使得发送错误帧。另外,帧解释部350在接收到错误帧的情况下,即在根据所接收到的帧的值而解释为成为错误帧的情况下,自此之后丢弃该帧,即中止帧的解释。

[0110] 接收ID判断部330接收从帧解释部350通知的ID域的值,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域之后的帧的各域的判定。接收ID判断部330将该判定结果通知给帧解释部350。

[0111] 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)。

[0112] 传送处理部310按照传送规则保持部370保持的传送规则,根据接收到的帧的消息ID,决定要传送的总线,将表示要传送的总线的总线信息、从帧解释部350通知的消息ID和数据通知给帧生成部320。此外,网关300不将从某总线接收到的错误帧传送到其他总线。

[0113] 传送规则保持部370保持表示各条总线的关于帧传送的规则的信息即传送规则。图7是示出了传送规则的一例的图。

[0114] 帧生成部320按照从帧解释部350通知的指示错误帧的发送的通知,构成错误帧,将错误帧通知给帧收发部360并使其发送该错误帧。另外,帧生成部320使用从传送处理部

310通知的消息ID和数据来构成帧,将帧以及总线信息通知给帧收发部360。

[0115] [1.7传送规则例]

[0116] 图7表示如上述那样网关300保有的传送规则的一例。该传送规则使传送源的总线、传送目的地的总线和传送对象的ID(消息ID)相关联。图7中的“*”表示不管消息ID如何都进行帧的传送这一情况。另外,该图中的“-”表示没有传送对象的帧这一情况。该图的例子示出了从总线500a接收的帧被设定为不管消息ID如何都向总线500b以及总线500c进行传送。另外,示出了从总线500b接收的帧被设定为向总线500c传送全部帧,而向总线500a仅传送消息ID为“3”的帧。另外,示出了从总线500c接收的帧被设定为既不向总线500a也不向总线500b进行传送。

[0117] [1.8ECU400a的构成]

[0118] 图8是ECU400a的构成图。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,该各功能通过ECU400a中的通信线路、执行存储器所保存的控制程序的处理器或数字电路等来实现。

[0119] 帧收发部460相对于总线500a收发遵循CAN协议的帧。从总线500a逐比特地接收帧,并传送给帧解释部450。另外,将从帧生成部420收到了通知的帧的内容发送到总线500a。

[0120] 帧解释部450从帧收发部460接收帧的值,进行解释以使得向由CAN协议规定的帧格式的各领域进行映射。ID域和判断出的值被传送给接收ID判断部430。帧解释部450根据从接收ID判断部430通知的判定结果,决定是将ID域的值和ID域之后出现的数据域传送给帧处理部410还是在收到该判定结果之后中止帧的接收(即中止作为该帧的解释)。另外,帧解释部450在判断为是未遵循CAN协议的帧的情况下,向帧生成部420进行通知,以使得发送错误帧。另外,帧解释部450在接收到错误帧的情况下,即在根据所接收到的帧的值而解释为成为错误帧的情况下,自此之后丢弃该帧,即中止帧的解释。

[0121] 接收ID判断部430接收从帧解释部450通知的ID域的值,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域之后的帧的各域的判定。接收ID判断部430将该判定结果通知给帧解释部450。

[0122] 接收ID列表保持部440保存ECU400a接收的ID(消息ID)的列表即接收ID列表。图9是示出了接收ID列表的一例的图。

[0123] 帧处理部410根据接收到的帧的数据,按每个ECU进行与不同的功能相关的处理。例如,与发动机401连接的ECU400a具备在时速超过了30km的状态下门开着的状态时鸣响警报声的功能。ECU400a具有例如用于鸣响警报声的扬声器等。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),基于从发动机401取得的时速来进行在一定条件下鸣响警报声的处理等。

[0124] 数据取得部470取得表示与ECU连接的设备、传感器等的状态的数据,通知给帧生成部420。

[0125] 帧生成部420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,将错误帧通知给帧收发部460并使其发送该错误帧。另外,帧生成部420对从数据取得部470通知的数据的值附加预先确定的消息ID来构成帧,并通知给帧收发部460。

[0126] 此外,ECU400b~400d也具备与上述的ECU400a基本上同样的构成。但是,接收ID列表保持部440所保持的接收ID列表可能会成为按各个ECU而不同的内容。ECU400b保存图9所例示的接收ID列表,ECU400c以及ECU400d保存图5所例示的接收ID列表。另外,帧处理部410的处理内容按各个ECU而不同。例如,ECU400c中的帧处理部410的处理内容包括与在未施加制动的状况下打开门时鸣响警报声的功能相关的处理。例如,ECU400b以及ECU400d中的帧处理部410不进行特别的处理。此外,各ECU也可以具备在此例示的功能以外的功能。此外,关于ECU400a~400d分别发送的帧的内容,在后面使用图10~图13进行说明。

[0127] [1.9接收ID列表例2]

[0128] 上述的图9是表示在ECU400a和ECU400b的各ECU中保持的接收ID列表的一例的图。该图所例示的接收ID列表用于选择性地接收包含ID(消息ID)的值为“1”、“2”和“3”的某一个的消息ID的帧并进行处理。例如,若在ECU400a的接收ID列表保持部440中保持有图9的接收ID列表,则关于消息ID不为“1”、“2”和“3”的任一个的帧,中止帧解释部450中的ID域之后的帧的解释。

[0129] [1.10与发动机相关的ECU400a的发送帧例]

[0130] 图10是表示从与发动机401连接的ECU400a发送的帧的ID(消息ID)以及数据域(数据)的一例的图。ECU400a发送的帧的消息ID为“1”。数据表示时速(km/小时),取最低0(km/小时)~最高180(km/小时)的范围内的值,数据长为1个字节。从图10的上面的行向下面的行例示了与从ECU400a逐次发送的各帧对应的各消息ID以及数据,示出了从0km/小时起每次加速1km/小时的情形。

[0131] [1.11与制动器相关的ECU400b的发送帧例]

[0132] 图11是表示从与制动器402连接的ECU400b发送的帧的ID(消息ID)以及数据域(数据)的一例的图。ECU400b发送的帧的消息ID为“2”。数据以比例(%)的方式表示制动的施加情况,数据长为1个字节。对于该比例,将完全没有施加制动的状态设为0(%),将最大限度地施加制动的状态设为100(%)。从图11的上面的行向下面的行例示了与从ECU400b逐次发送的各帧对应的各消息ID以及数据,示出了从100%逐渐减弱制动的情况。

[0133] [1.12与门开闭传感器相关的ECU400c的发送帧例]

[0134] 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)以及数据域(数据)的一例的图。ECU400c发送的帧的消息ID为“3”。数据表示门的开关状态,数据长为1个字节。对于数据的值,开着门的状态为“1”,关着门的状态为“0”。从图12的上面的行向下面的行例示了与从ECU400c逐次发送的各帧对应的各消息ID以及数据,示出了从开着门的状态接着转变为关闭的状态的情形。

[0135] [1.13与窗开闭传感器相关的ECU400d的发送帧例]

[0136] 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)以及数据域(数据)的一例的图。ECU400d发送的帧的消息ID为“4”。数据以比例(%)的方式表示窗的开关状态,数据长为1个字节。对于该比例,将窗完全关着的状态设为0(%),将窗完全开着的状态设为100(%)。从图13的上面的行向下面的行例示了与从ECU400d逐次发送的各帧对应的各消息ID以及数据,示出了从关着窗的状态逐渐打开的情形。

[0137] [1.14不正常检测ECU100a的构成]

[0138] 图14是不正常检测ECU100a的构成图。不正常检测ECU100a构成为包括帧收发部

160、帧解释部150、不正常帧检测部130、正规ID列表保持部120、不正常检测计数器保持部110和帧生成部140。这些各构成要素是功能性的构成要素,该各功能通过不正常检测ECU100a中的通信线路、执行存储器所保存的控制程序的处理器或数字电路等来实现。此外,不正常检测ECU100b也具有基本上同样的构成,但正规ID列表保持部120保持的列表信息(正规ID列表)的内容按不正常检测ECU100a和不正常检测ECU100b而不同。

[0139] 帧收发部160相对于总线500a收发遵循CAN协议的帧。即,帧收发部160在总线上的帧的发送开始了的情况下接收帧,也就是说作为接收部进行工作,另外,向总线发送错误帧等,也就是说作为发送部进行工作。即,帧收发部160从总线500a逐比特地接收帧,并传送给帧解释部150。另外,将从帧生成部140收到了通知的帧的内容发送到总线500a。

[0140] 帧解释部150从帧收发部160接收帧的值,进行解释以使得向由CAN协议规定的帧格式的各域进行映射。ID域和判断出的值被传送给不正常帧检测部130。另外,帧解释部150在判断为是未遵循CAN协议的帧的情况下,向帧生成部140进行通知,以使得发送错误帧。另外,帧解释部150在接收到错误帧的情况下,即在根据所接收到的帧的值而解释为成为错误帧的情况下,自此之后丢弃该帧,即中止帧的解释。

[0141] 不正常帧检测部130接收从帧解释部150通知的ID域的值,判定ID域的值是否符合表示不正常的预定条件。即,不正常帧检测部130判定所接收到的帧的预定域的内容是否符合表示不正常的预定条件,也即作为判定部发挥功能。该表示不正常的预定条件是ID域的值未记载在正规ID列表保持部120保持的消息ID的列表中这一条件。即,按照正规ID列表保持部120保持的消息ID的列表,进行所通知的ID域的值(消息ID)是否不正常的判定。在接收到未记载在该列表(即后述的正规ID列表)中的消息ID的情况下,为了使不正常的检测次数递增,将所接收到的消息ID通知给不正常检测计数器保持部110。另外,在接收到未记载在正规ID列表中的消息ID的情况下,为了发送错误帧而向帧生成部140进行通知。另外,在不正常的检测次数达到了一定次数以上的情况下,从不正常检测计数器保持部110接收通知,并向帧生成部140进行通知,以使得发送表示存在发布该消息ID的不正常ECU这一情况的示错消息(帧)。示错消息的消息ID被预先确定,头单元200接收该消息ID的消息(帧)并进行示错。关于该示错消息,方便起见省略说明,但示错消息的消息ID登记在网关300以及头单元200保持的接收ID列表以及后述的正规ID列表中。但是,在图15、图16中省略了关于示错消息的消息ID。

[0142] 正规ID列表保持部120保持对在车载网络系统10中会在总线500a上发送的帧所包含的消息ID进行了预先规定的列表即正规ID列表(参照图15、图16)。

[0143] 不正常检测计数器保持部110保持有助于按各个消息ID对检测次数进行计数的不正常检测计数器,当从不正常帧检测部130通知了消息ID时,使相应的不正常检测计数器增加(increment)。在不正常检测计数器达到了一定数(预定次数)以上的情况下,向不正常帧检测部130通知超过了一定数这一情况。在此所说的一定数(预定次数)的一例是与CAN协议中的发送错误计数器的处理规则对应而确定的值。在CAN协议中,ECU每次由于错误帧而阻止发送时,发送错误计数器都计数增加8。并且,规定为:如果作为其结果是发送节点中的发送错误计数器计数增加到128,则发送节点转变到消极(passive)状态而不再进行帧发送。因此,如果将比 $128/8 (= 16)$ 大的17设定为该一定数,则成为:在推定为存在无视了CAN协议中的发送错误计数器所涉及的规则的发送节点(不正常ECU)的情况下,从不正常检测

ECU100a发送示错消息。此外,在发送不正常帧的不正常ECU遵循CAN协议中的发送错误计数器所涉及的规则的情况下,通过由不正常检测ECU100a进行的错误帧的发送,不正常ECU的发送错误计数器增加8。该情况下,当通过反复进行不正常帧的发送从而不正常ECU的发送错误计数器上升到128时,不正常ECU会转变到消极状态,停止由不正常ECU进行的不正常帧的发送。

[0144] 帧生成部140按照从帧解释部150通知的指示错误帧的发送的通知,构成错误帧,将错误帧通知给帧收发部160并使其发送该错误帧。另外,帧生成部140按照从不正常帧检测部130通知的指示错误帧的发送的通知,构成错误帧,将错误帧通知给帧收发部160并使其发送该错误帧。进而,帧生成部140按照从不正常帧检测部130通知的指示示错消息的发送的通知,将示错消息通知给帧收发部160并使其发送该示错消息。

[0145] [1.15不正常检测ECU100a的正规ID列表例]

[0146] 图15是示出了在不正常检测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列表示出了包含ID(消息ID)的值为“1”、“2”和“3”的任一个的消息ID的帧能够在总线500a中传播这一情况。

[0147] [1.16不正常检测ECU100b的正规ID列表例]

[0148] 图16是示出了在不正常检测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列表示出了包含ID(消息ID)的值为“1”、“2”、“3”和“4”的任一个的消息ID的帧能够流在总线500b中传播这一情况。

[0149] [1.17不正常检测计数器保存列表例]

[0150] 图17是表示各个消息ID的不正常检测计数器的状态的一例的图。该图的例子示出了仅消息ID为“4”的不正常检测计数器检测到一次不正常,关于其他的消息ID则一次都没有检测到。即,该例子示出了如下情况:不正常检测ECU100a检测到一次发送了本来不应该在总线500a中传播的消息ID“4”的消息(帧),使与该消息ID“4”对应的不正常检测计数器增加一。

[0151] [1.18与不正常帧的检测相关的时序]

[0152] 以下,关于在具备上述结构的车载网络系统10的总线500a上连接有不正常ECU的情况,对与总线500a连接的不正常检测ECU100a、ECU400a、ECU400b、网关300等的工作进行说明。

[0153] 图18是表示不正常检测ECU100a检测到不正常帧(消息),并阻止由其他ECU进行应对该不正常帧的处理的工作例的时序图。在该图中,示出了不正常ECU向总线500a发送消息ID为“4”且数据域(数据)为“255(0xFF)”的数据帧的情况下的例子。在此的各时序意味着各种装置中的各处理步骤(step)。

[0154] 首先,不正常ECU开始消息ID为“4”且数据为“255(0xFF)”的数据帧的发送(时序S1001)。构成帧的各比特的值按照上述的数据帧格式,按SOF、ID域(消息ID)这样的顺序逐次被送出到总线500a上。

[0155] 在不正常ECU向总线500a送完了到ID域(消息ID)为止的数据时,不正常检测ECU100a、ECU400a、ECU400b以及网关300分别接收消息ID(时序S1002)。

[0156] ECU400a、ECU400b以及网关300分别使用所保持的接收ID列表来检查消息ID(时序S1003)。此时,不正常检测ECU100a使用所保持的正规ID列表来检查消息ID(时序S1004)。

即,不正常检测ECU100a判定被发送来的帧中的ID域的内容是否符合表示不正常的预定条件(未登记在正规ID列表中)。

[0157] 在时序S1003中,ECU400a以及ECU400b由于分别保持的接收ID列表中不包含“4”(参照图9),所以结束接收。也即是,不再进行不正常ECU继续发送的帧的解释,不再进行应对帧的处理。另外,在时序S1003中,网关300由于所保持的接收ID列表中不包含“4”(参照图5),所以继续接收。另外,在时序S1004中,不正常检测ECU100a由于所保持的正规ID列表中不包含“4”,所以判断为是不正常的消息ID,接着开始错误帧的发布准备(时序S1005)。

[0158] 接着时序S1003,网关300继续帧的接收。例如,在不正常检测ECU100a正在进行错误帧的发布准备的期间,从不正常ECU向总线500a上逐次送出ID域之后的部分即RTR、控制域(IDE、r、DLC),接着逐比特地送出数据域。网关300接收该RTR、控制域(IDE、r、DLC),接着开始数据域的接收(时序S1006)。

[0159] 接着,错误帧的发布准备结束,不正常检测ECU100a发送错误帧(时序S1007)。该错误帧的发送在不正常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。在该工作例中,在数据域的中途进行。通过开始该错误帧的发送,在总线500a中从不正常ECU正在发送的帧的数据域的中途部分会被错误帧(优先的显性的位串)覆写。

[0160] 接收到在时序S1007中发送的错误帧的网关300,在数据域的接收中途中止不正常ECU发送出的帧的接收(时序S1008)。也即,网关300因为来自不正常ECU的数据域被错误帧覆写而检测到错误帧,所以不继续不正常ECU发送出的帧的接收。

[0161] 不正常检测ECU100a使成为发送错误帧的对象的数据帧的消息ID“4”所对应的不正常检测计数器增加(时序S1009)。

[0162] 在作为增加后的结果是与消息ID“4”对应的不正常检测计数器达到了17以上的情况下,不正常检测ECU100a发送通知示错的帧(示错消息),以使得被头单元200接收(时序S1010)。作为其结果,由头单元200的帧处理部220进行用于示错的处理,经由LCD等报告错误。此外,错误的报告除了通过向LCD等进行显示之外,还可以通过声音输出、发光等来进行。

[0163] [1.19实施方式1的效果]

[0164] 实施方式1中示出的不正常检测ECU,使用正规ID列表对帧的ID域判定所发送来的帧(数据帧)是否为不正常帧。由此,能够根据数据帧中的ID域来对不正常进行判定,因此,能够阻止在既有的节点(即不正常检测ECU以及不正常ECU以外的ECU)中对不正常帧进行解释而执行应对该帧的处理。另外,仅通过接收到数据帧的继开头的SOF之后的ID域为止就能够进行判定,因此与接收数据帧的后部等来进行判定的情况相比,能够抑制总线的通信量。

[0165] 另外,不正常检测ECU使用不正常检测计数器对发送了错误帧的次数进行计数,由此,如果通过接收错误帧而发送不正常的消息ID的节点中的发送错误计数器遵循CAN协议,则能够对达到应该转变到消极状态的上限值这一情况进行检测。由此,能够判定发送不正常的消息ID的节点是否遵照了CAN协议的错误计数器的规格。

[0166] 另外,通过仅将进行不正常帧的判定的节点设为不正常检测ECU,能够将对既有的网络结构的影响抑制为最小限度,能够抑制系统整体的处理量、耗电量。

[0167] (实施方式2)

[0168] 以下,作为本公开的实施方式,对包含实现如下的不正常应对方法的不正常检测

ECU的车载网络系统11进行说明,在该不正常应对方法中,基于按各个消息ID所允许的数据范围,阻止在其他节点(ECU)中执行基于不正常帧的处理。

[0169] [2.1车载网络系统11的整体构成]

[0170] 图19是表示实施方式2涉及的车载网络系统11的整体构成的图。车载网络系统11是对实施方式1中示出的车载网络系统10的一部分进行了变形而得到的。车载网络系统11构成为包括总线500a、500b、不正常检测ECU2100a、2100b、头单元200、网关300、以及通过各种设备连接的ECU400a~400d等ECU这种连接于总线的各节点。对于车载网络系统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,标注相同的附图标记而省略说明。

[0171] 不正常检测ECU2100a、2100b分别与总线500a、总线500b连接,是具有判定从ECU400a~400d等发送的帧是否不正常,如果不正常则发送错误帧的功能的ECU。

[0172] [2.2不正常检测ECU2100a的构成]

[0173] 图20是不正常检测ECU2100a的构成图。不正常检测ECU2100a构成为包括帧收发部160、帧解释部2150、不正常帧检测部2130、数据范围列表保持部2120、不正常检测计数器保持部110和帧生成部140。这些各构成要素是功能性的构成要素,该各功能通过不正常检测ECU2100a中的通信线路、执行存储器所保存的控制程序的处理器或数字电路等来实现。不正常检测ECU2100a是对实施方式1中示出的不正常检测ECU100a的一部分进行了变形而得到的,对于具有与实施方式1同样的功能的构成要素,标注相同的附图标记而省略说明。此外,不正常检测ECU2100b也具备与不正常检测ECU2100a同样的构成。

[0174] 帧解释部2150是对实施方式1中示出的帧解释部150进行了变形而得到的,从帧收发部160接收帧的值,进行解释以使得向由CAN协议规定的帧格式的各领域进行映射。在判断为帧是数据帧的情况下,数据域和判断出的值(数据)与ID域的ID(消息ID)一起传送给不正常帧检测部2130。另外,帧解释部2150在判断为是未遵循CAN协议的帧的情况下,向帧生成部140进行通知,以使得发送错误帧。另外,帧解释部2150在接收到错误帧的情况下,即在根据所接收到的帧的值而解释为成为错误帧的情况下,自此之后丢弃该帧,即中止帧的解释。

[0175] 不正常帧检测部2130是对实施方式1中示出的不正常帧检测部130进行了变形而得到的,接收从帧解释部2150通知的消息ID和数据域的值(数据),判定这些值是否符合表示不正常的预定条件。即,不正常帧检测部2130判定所接收到的帧中的预定域的内容是否符合表示不正常的预定条件,即作为判定部发挥功能。该表示不正常的预定条件是数据未落入到在数据范围列表保持部2120所保持的数据范围列表中与消息ID关联记载的数据范围内这一条件。不正常帧检测部2130按照数据范围列表保持部2120所保持的确定了各个消息ID的数据范围的列表即数据范围列表,进行是否不正常的判定。不正常帧检测部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,为了使不正常的检测次数增加而将所接收到的消息ID通知给不正常检测计数器保持部110。对于在该不正常的检测次数达到了一定次数以上的情况下用于发送示错消息以使得由头单元200接收的控制,与实施方式1中说明的一样,因此省略在此的说明。另外,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进行通知,以使得发送错误帧。

[0176] 数据范围列表保持部2120保持对在车载网络系统11中在总线上发送的数据帧所包含的数据(数据域的值)所允许的范围进行了预先规定的列表即数据范围列表(参照图21)。

[0177] [2.3数据范围列表例]

[0178] 图21是示出了在不正常检测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。该数据范围列表是使各ID(消息ID)和作为该消息ID的数据帧中的数据域的值(数据)而允许的数据范围相关联的列表。在图21的例子中,关于消息ID为“1”的数据帧,将数据范围“0~180”设为正常,关于消息ID为“2”或“4”的数据帧,将数据范围“0~100”设为正常,关于消息ID为“3”的数据帧,将数据范围“0、1”设为正常。

[0179] [2.4与不正常帧的检测相关的时序]

[0180] 以下关于在具备上述结构的车载网络系统11的总线500a上连接有不正常ECU的情况,对与总线500a连接的不正常检测ECU2100a、ECU400a、ECU400b、网关300等的工作进行说明。

[0181] 图22以及图23是表示不正常检测ECU2100a检测到不正常帧(消息),阻止由其他ECU进行应对该不正常帧的处理的工作例的时序图。在图22以及图23中,与实施方式1中示出的图18的情况同样,示出了不正常ECU向总线500a发送消息ID为“4”且数据域(数据)为“255(0xFF)”的数据帧的情况下的例子。对与实施方式1中示出的时序相同的时序标注相同的附图标记,在此简化说明。

[0182] 首先,不正常ECU开始不正常数据帧的发送(时序S1001)。不正常检测ECU2100a、ECU400a、ECU400b以及网关300分别接收消息ID(时序S1002)。ECU400a、ECU400b以及网关300分别使用所保持的接收ID列表来检查消息ID(时序S1003)。ECU400a以及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。网关300由于所保持的接收ID列表中不包含“4”(参照图5),所以继续接收并进行数据域的接收(时序S1006a)。同样地,不正常检测ECU2100a也进行数据域的接收(时序S1006a)。

[0183] 接着时序S1006a,不正常检测ECU2100a使用数据范围列表(参照图21)来检查数据域的数据(时序S2001)。即,不正常检测ECU2100a判定所发送来的帧中的ID域的内容是否符合表示不正常的预定条件(未落入数据范围列表所记载的数据的范围内)。由于在数据范围列表中未记载有与ID“4”对应的“255(0xFF)”的值,所以不正常检测ECU2100a判断为是不正常的数据帧,接着开始错误帧的发布准备(时序S1005)。

[0184] 在不正常检测ECU2100a正在进行错误帧的发布准备的期间,从不正常ECU向总线500a上逐比特地送出数据域之后的部分即CRC域(CRC序列以及CRC定界符)。网关300开始该CRC域的接收(时序S2002)。

[0185] 接着,错误帧的发布准备结束,不正常检测ECU2100a发送错误帧(时序S1007)。通过开始该错误帧的发送,在总线500a上从不正常ECU正在发送的帧的CRC序列的中途部分会被错误帧(优先的显性的位串)覆写。

[0186] 接收到在时序S1007中发送的错误帧的网关300,在包含CRC序列的CRC域的接收中途中止不正常ECU发送出的数据帧的接收(时序S2003)。也即是,网关300因为来自不正常ECU的CRC序列被错误帧覆写而检测到错误帧,所以不继续不正常ECU发送出的数据帧的接收。

[0187] 不正常检测ECU2100a使成为发送错误帧的对象的数据帧的ID“4”所对应的不正常检测计数器增加(时序S1009)。在作为增加后的结果是与ID“4”对应的不正常检测计数器达到了17以上的情况下,不正常检测ECU2100a发送示错消息(时序S1010)。

[0188] [2.5实施方式2的效果]

[0189] 实施方式2中示出的不正常检测ECU,使用数据范围列表对帧(数据帧)的ID域以及数据域判定所发送来的帧是否为不正常帧。由此,能够通过数据帧中的ID域和数据域的组合来判定不正常,因此能够阻止在既有的ECU(即不正常检测ECU以及不正常ECU以外的ECU)中对不正常帧进行解释并执行应对该帧的处理。另外,仅通过接收到数据帧的数据域为止就能够进行判定,因此与接收数据帧的后部来进行判定的情况相比,能够抑制总线的通信量。

[0190] 另外,不正常检测ECU使用不正常检测计数器对发送了错误帧的次数进行计数,由此,如果通过接收错误帧而发送不正常的消息ID的节点中的发送错误计数器遵循CAN协议,则能够对达到应该转变到消极状态的上限值这一情况进行检测。由此,能够判定发送不正常的消息ID的节点是否遵照了CAN协议的错误计数器的规格。

[0191] 另外,通过仅将进行不正常帧的判定的节点设为不正常检测ECU,能够将对既有的网络结构的影响抑制为最小限度,能够抑制系统整体的处理量、耗电量。

[0192] (实施方式3)

[0193] 以下,作为本公开的实施方式,对包含实现如下的不正常应对方法的不正常检测ECU的车载网络系统12进行说明,在该不正常应对方法中,使用根据消息ID、数据以及计数器值而算出的消息认证码(MAC:Message Authentication Code),阻止在其他节点(ECU)中执行基于不正常帧的处理。

[0194] [3.1车载网络系统12的整体构成]

[0195] 图24是表示实施方式3涉及的车载网络系统12的整体构成的图。车载网络系统12是对实施方式1中示出的车载网络系统10的一部分进行了变形而得到的。车载网络系统12构成为包括总线500a、500b、不正常检测ECU3100a、3100b、头单元200、网关300、以及与各种设备连接的ECU3400a~3400d等ECU这种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,标注相同的附图标记而省略说明。

[0196] 不正常检测ECU3100a、3100b分别与总线500a、总线500b连接,是具有判定从ECU3400a~3400d等发送的帧是否不正常,如果不正常则发送错误帧的功能的ECU。

[0197] ECU3400a~3400d与某一总线连接,另外,ECU3400a~3400d分别与发动机401、制动器402、门开闭传感器403、窗开闭传感器404连接。ECU3400a~3400d分别取得连接着的设备(发动机401等)的状态,定期地向网络(即总线)发送表示状态的数据帧。对所发送的数据帧的数据域,赋予根据消息ID、数据值和每次发送都增加的计数器值而通过计算导出的消息认证码(MAC)。

[0198] [3.2ECU3400a的构成]

[0199] 图25是ECU3400a的构成图。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,该各功能通过ECU3400a中的通信线路、执行存储器所保存的控制程序的处理器或数字电路等来实现。ECU3400a是对实施方式1中示出的ECU400a的一部分进行了变形而得到的,对于具有与实施方式1同样的功能的构成要素,标注相同的附图标记而省略说明。

[0200] 帧生成部3420是对实施方式1中示出的帧生成部420的一部分进行了变形而得到

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,将错误帧通知给帧收发部460并使其发送该错误帧。另外,帧生成部3420将从数据取得部470通知的数据的值和预先设定的消息ID通知给MAC生成部3410,接收所算出的MAC。帧生成部3420以使得包含预先设定的消息ID、从数据取得部470通知的数据的值、和从MAC生成部3410接收到的MAC的方式构成帧(参照图26),并通知给帧收发部460。

[0201] MAC生成部3410使用由MAC密钥保持部3430保持的MAC密钥,对结合了从帧生成部3420通知的消息ID和数据的值、与由计数器保持部3440保持的计数器值而得到的值(结合值)算出MAC(通过计算而导出),将作为该算出的结果的MAC通知给帧生成部3420。在此,作为MAC的计算方法,采用HMAC(Hash-based Message Authentication Code,基于散列运算的消息认证码)(参照非专利文献2),对上述结合值,以进行填充直到预定的块量(例如4个字节)而成的值,使用MAC密钥进行计算,将得出的计算结果的开头4个字节作为MAC值。此外,在此,为了算出MAC而使用的结合值,使用了消息ID、数据的值和由计数器保持部3440保持的计数器值,但也可以使用这三个中的任意一个或两个的组合来算出MAC。

[0202] MAC密钥保持部3430保持为了计算MAC所需的MAC密钥。

[0203] 计数器保持部3440保持为了计算MAC所需的计数器值。此外,该计数器值每次在帧收发部460中正常发送了数据帧时增加。

[0204] 此外,ECU3400b~3400d分别是对实施方式1中示出的ECU400b~400d的一部分进行了变形而得到的,具备与上述的ECU3400a基本上同样的构成。但是,接收ID列表保持部440所保持的接收ID列表可以成为按各个ECU而不同的内容。例如ECU3400a以及ECU3400b保持图9所例示的接收ID列表,ECU3400c以及ECU3400d保持图5所例示的接收ID列表。另外,帧处理部410的处理内容如实施方式1所示按各个ECU而不同。以下,使用图26~图29对ECU3400a~3400d分别发送的帧的内容进行说明。

[0205] [3.3与发动机相关的ECU3400a的发送帧例]

[0206] 图26是表示从与发动机401连接的ECU3400a发送的数据帧的ID(消息ID)以及数据域(数据)的一例的图。ECU3400a发送的帧的消息ID为“1”。在该图中,按每个字节而用空格区分表示数据,开头的1个字节表示时速(km/小时),接着的1个字节表示计数器值,接着的4个字节表示MAC。此外,在图26的例子中MAC由16进制数来标记。开头1个字节的时速(km/小时)取最低0(km/小时)~最高180(km/小时)的范围的值。从图26的上面的行向下面的行例示了与从ECU3400a逐次发送的各帧对应的各消息ID以及数据,示出了计数器值逐渐增加、时速从0km/小时起每次加速1km/小时的情形。

[0207] [3.4与制动器相关的ECU3400b的发送帧例]

[0208] 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)以及数据域(数据)的一例的图。ECU3400b发送的帧的消息ID为“2”。在该图中,按每个字节而用空格区分表示数据,开头的1个字节以比例(%)的方式表示制动的施加情况,接着的1个字节表示计数器值,接着的4个字节表示MAC。此外,在图27的例子中,MAC由16进制数来标记。对于开头1个字节的制动的施加情况,将完全没有施加制动的状态设为0(%),将最大限度地施加制动的状态设为100(%)。从图27的上面的行向下面的行例示了与从ECU3400b逐次发送的各帧对应的各消息ID以及数据,示出了如下情形:计数器值逐渐增加,对于制动而言从100%逐渐减弱制动。

[0209] [3.5与门开闭传感器相关的ECU3400c的发送帧例]

[0210] 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)以及数据域(数据)的一例的图。ECU3400c发送的帧的消息ID为“3”。在该图中,按每个字节而用空格区分表示数据,开头的1个字节表示门的开关状态,接着的1个字节表示计数器值,接着的4个字节表示MAC。此外,在图28的例中MAC由16进制数来标记。对于开头1个字节的门的开关状态,将开着门的状态设为“1”,将关着门的状态设为“0”。从图28的上面的行向下面的行例示了与从ECU3400c逐次发送的各帧对应的各消息ID以及数据,示出了计数器值逐渐增加、从开着门的状态接着向关闭的状态转变的情形。

[0211] [3.6与窗开闭传感器相关的ECU3400d的发送帧例]

[0212] 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)以及数据域(数据)的一例的图。ECU3400d发送的帧的消息ID为“4”。在该图中,按每个字节而用空格区分表示数据,开头的1个字节以比例(%)的方式表示窗的开关状态,接着的1个字节表示计数器值,接着的4个字节表示MAC。此外,在图29的例子中MAC由16进制数来标记。对于开头1个字节的窗的开关状态,将完全关着窗的状态设为0(%),将完全开着窗的状态设为100(%)。从图29的上面的行向下面的行例示了与从ECU3400d逐次发送的各帧对应的各消息ID以及数据,示出了计数器值逐渐增加、从关着窗的状态逐渐打开的情形。

[0213] [3.7不正常检测ECU3100a的构成]

[0214] 图30是不正常检测ECU3100a的构成图。不正常检测ECU3100a包括帧收发部160、帧解释部3150、不正常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和不正常检测计数器保持部110。这些各构成要素是功能性的构成要素,该各功能通过不正常检测ECU3100a中的通信线路、执行存储器所保存的控制程序的处理器或数字电路等来实现。不正常检测ECU3100a是对实施方式1中示出的不正常检测ECU100a的一部分进行了变形而得到的,对于具有与实施方式1同样的功能的构成要素,标注相同的附图标记而省略说明。此外,不正常检测ECU3100b也是同样的构成。

[0215] 帧解释部3150是对实施方式1中示出的帧解释部150进行了变形而得到的,从帧收发部160接收帧的值,进行解释以使得向由CAN协议规定的帧格式的各领域进行映射。在判断为帧是数据帧的情况下,数据域和判断出的值(数据)与ID域的ID(消息ID)一起传送给不正常MAC检测部3130。另外,帧解释部3150在判断为是未遵循CAN协议的帧的情况下,向帧生成部140进行通知,以使得发送错误帧。另外,帧解释部3150在接收到错误帧的情况下,即在根据所接收到的帧的值而解释为成为错误帧的情况下,自此之后丢弃该帧,即中止帧的解释。

[0216] 不正常MAC检测部3130具有接收从帧解释部3150通知的消息ID和数据域的值(数据)来验证数据域中的MAC的功能。不正常MAC检测部3130将通知来的消息ID以及数据域的值通知给MAC生成部3170,从MAC生成部3170取得所生成的MAC。不正常MAC检测部3130判定数据域的数据是否符合表示不正常的预定条件。即,不正常MAC检测部3130判定所接收到的帧中的预定域的内容是否符合表示不正常的预定条件,也即作为判定部发挥功能。该表示不正常的预定条件是所设定的验证处理步骤(包括MAC的生成、MAC的比较等的步骤)中的验证失败、即数据所包含的MAC与由MAC生成部3170生成的MAC不同这一条件。不正常MAC检测部3130通过对从MAC生成部3170取得的MAC和数据域中的MAC进行比较,进行是否不正常的判定(即MAC的验证)。在两个MAC的值的比较结果不一致的情况下,为了使不正常的检测次

数增加而将接收到的消息ID通知给不正常检测计数器保持部110。关于在该不正常的检测次数达到了一定次数以上的情况下用于发送示错消息以使得被头单元200接收的控制,与实施方式1中说明的一样,因此省略在此的说明。另外,在两个MAC的值的比较结果不一致的情况下,向帧生成部140进行通知,以使得发送错误帧。在MAC值的比较结果一致的情况下,向MAC生成部3170进行通知,以使得计数器保持部3190保持的与消息ID对应的计数器值增加。

[0217] MAC生成部3170使用从不正常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取得对应的计数器值。MAC生成部3170针对从不正常MAC检测部3130通知的数据域的值(开头1个字节的值)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密钥来算出(通过计算而导出)MAC,将算出的MAC通知给不正常MAC检测部3130。此外,在不正常检测ECU3100a、3100b以及ECU3400a~3400d的任一方中,使用MAC密钥来算出MAC的算法使用相同的算法。

[0218] MAC密钥保持部3180使用于计算MAC所需的MAC密钥与各个消息ID相关联地进行保持。该MAC密钥保持部3180保持的MAC密钥是按关联的各个消息ID而不同的值。此外,当设想一个发送节点发送多个消息ID各自的帧时,在ECU以及不正常检测ECU中使用的MAC密钥也可以设为按各个发送节点而不同的密钥。另外,MAC密钥例如也可以设为对相同总线上发送的帧使用相同的值,也可以设为即使在不同总线上也为相同的密钥(值),也可以设为按每台车辆而相同的密钥,也可以设为按相同的车型而相同的密钥,也可以设为按相同的制造商而相同的密钥,也可以设为即使是不同的制造商也为相同的密钥。

[0219] 计数器保持部3190按各个消息ID保持用于计算MAC值所需的计数器值。该计数器值在正常接收到帧的情况(即在不正常MAC检测部3130中比较的两个MAC一致的情况)下增加。

[0220] [3.8计数器值的例子]

[0221] 图31是表示在计数器保持部3190中保持的各个消息ID的计数器值的一例的图。在该图中,消息ID为“1”的计数器示出了1次,消息ID为“2”的计数器示出了10次,消息ID为“3”的计数器示出了15次,消息ID为“4”的计数器示出了100次。与该各消息ID对应的计数器值示出了包含该消息ID的帧被正常接收的次数。

[0222] [3.9与不正常帧的检测相关的时序]

[0223] 以下,关于在具备上述结构的车载网络系统12的总线500a上连接有不正常ECU的情况,对与总线500a连接的不正常检测ECU3100a、ECU3400a、ECU3400b、网关300等的工作进行说明。

[0224] 图32以及图33是表示不正常检测ECU3100a检测到不正常帧(消息),阻止由其他ECU进行应对该不正常帧的处理的工作例的时序图。在图32以及图33中,与实施方式1中示出的图18以及实施方式2中示出的图22以及图23的情况同样,示出了不正常ECU连接于总线500a的例子。该不正常ECU发送消息ID为“4”且数据域(数据)为“0xFF FF FFFFFFFF”(6个字节)的数据帧。对与实施方式1或2中示出的时序相同的时序标注相同的附图标记,在此简化说明。

[0225] 首先,不正常ECU开始上述的不正常数据帧的发送(时序S1001a)。不正常检测ECU3100a、ECU3400a、ECU3400b以及网关300分别接收消息ID(时序S1002)。ECU3400a、

ECU3400b以及网关300分别使用所保持的接收ID列表来检查消息ID(时序S1003)。ECU3400a以及ECU3400b由于分别保持的接收ID列表中不包含“4”(参照图9),所以结束接收。网关300由于所保持的接收ID列表中包含“4”(参照图5),所以继续接收并进行数据域的接收(时序S1006a)。同样地,不正常检测ECU3100a也进行数据域的接收(时序S1006a)。

[0226] 接着时序S1006a,不正常检测ECU3100a对数据域中的数据所包含的MAC进行验证(检查)(时序S3001)。即,不正常检测ECU3100a判定所发送来的帧中的ID域的内容是否符合表示不正常的预定条件(MAC的验证失败)。不正常检测ECU3100a针对从不正常ECU发送的数据帧中的数据域的6个字节的数据“0xFFFFFFFF”,将后面4个字节的MAC与使用与消息ID“4”对应的MAC密钥和计数器而推算出的MAC进行比较,由此进行MAC的验证。因为该比较的结果不一致而验证失败,所以在不正常检测ECU3100a中判断为是不正常的帧,接着开始错误帧的发布准备(时序S1005)。

[0227] 在不正常检测ECU3100a正在进行错误帧的发布准备的期间,网关300开始CRC域的接收(时序S2002)。

[0228] 接着,错误帧的发布准备结束,不正常检测ECU3100a发送错误帧(时序S1007)。通过该错误帧的发送,在总线500a上从不正常ECU正在发送的帧的CRC序列的中途部分会被错误帧覆写。

[0229] 接收到在时序S1007中发送的错误帧的网关300,在包含CRC序列的CRC域的接收中途,中止不正常ECU发送出的数据帧的接收(时序S2003)。

[0230] 不正常检测ECU3100a使成为发送错误帧的对象的数据帧的ID“4”所对应的不正常检测计数器增加(时序S1009)。在作为增加后的结果是与ID“4”对应的不正常检测计数器达到了17以上的情况下,不正常检测ECU3100a发送示错消息(时序S1010)。

[0231] [3.10实施方式3的效果]

[0232] 实施方式3中示出的不正常检测ECU通过对包含在帧(数据帧)的数据域中的MAC进行验证来判定所发送的帧是否为不正常帧。由此,能够阻止在既有的ECU(即不正常检测ECU以及不正常ECU以外的ECU)中对不正常帧进行解释并执行应对该帧的处理。另外,仅通过接收到数据帧的数据域为止就能够进行判定,因此与接收数据帧的后部来进行判定的情况相比,能够抑制总线的通信量。

[0233] 另外,不正常检测ECU使用不正常检测计数器对发送了错误帧的次数进行计数,由此,如果通过接收错误帧而发送不正常的消息ID的节点中的发送错误计数器遵循CAN协议,则能够对达到应该转变到消极状态的上限值这一情况进行检测。由此,能够判定发送不正常的消息ID的节点是否遵照了CAN协议的错误计数器的规格。

[0234] 另外,通过仅将进行MAC的验证的节点设为不正常检测ECU,不需要通过不正常检测ECU以外的ECU进行验证,能够抑制系统整体的处理量、耗电量。

[0235] (其他实施方式等)

[0236] 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于此,在适当进行了变更、替换、附加、省略等的实施方式中也能够加以适用。例如,以下的变形例也包含在本公开的一个实施技术方案中。

[0237] (1)在上述实施方式中,示出了通过ECU400a~400d或ECU3400a~3400d定期地发送帧的例子,但也可以作为通知状态变化的事件而发送帧。例如,ECU也可以不是定期地发

送门的开关状态,而是仅在门的开关状态发生了变化的情况下才发送帧。另外,也可以设为ECU定期地发送帧、且在发生了状态变化时发送帧。

[0238] (2) 在实施方式3中,示出了根据数据值和计数器值来算出MAC的例子,但也可以仅根据数据值来算出MAC。另外,也可以仅根据计数器值来算出MAC。另外,帧所包含的MAC的大小并非限制于4个字节,也可以是按每次发送而不同的大小。同样,时速等数据值的大小以及计数器值的大小也并非限制于1个字节。另外,也可以不一定在帧中包含计数器值。

[0239] (3) 在实施方式3中,示出了每次发送都使计数器值增加的例子,但计数器值也可以是随着时刻而自动增加的值。另外,也可以取代计数器而使用时刻本身的值。即,若使得基于每次发送数据帧时都变化的变量(计数器、时刻等)来生成MAC,则可能会使得难以进行MAC的不正常解读。另外,在实施方式3中,设为了不正常检测ECU中的MAC生成部3170根据消息ID、数据域的开头1个字节和计数器保持部3190的计数器值来算出MAC值。但也可以取而代之而根据消息ID、数据域的开头1个字节和作为数据域的下一个字节的计数器值来算出MAC值。另外,也可以为对计数器保持部3190的计数器值进行更新,以使得与判定为并非不正常的数据域中的计数器值相匹配。

[0240] (4) 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。在扩展ID格式的情况下,由于用标准ID格式中的ID位置的基础ID和扩展ID共29比特来表示ID(消息ID),所以将该29比特的ID作为上述实施方式中的ID(消息ID)来处理即可。

[0241] (5) 在上述实施方式中,使算出MAC的算法为HMAC,但其也可以是CBC-MAC(Cipher Block Chaining Message Authentication Code:密码块链接消息认证码)、CMAC(Cipher-based MAC:基于密码的消息认证码)。另外,关于用于MAC计算的填充,只要零填充、ISO10126、PKCS#1、PKCS#5、PKCS#7、此外的块的数据大小(size)是计算所需要的填充方式,则任何方式都是可以的。另外,关于对4个字节等块的大小的变更方法,也可以在开头、最末尾以及中间的任一个部分进行填充。另外,用于算出MAC的数据也可以不是连续的数据(例如4个字节的连续数据),也可以按照特定规则而逐个比特收集并结合。

[0242] (6) 在上述实施方式中,作为遵循CAN协议进行通信的网络通信系统的例子而示出了车载网络。本公开涉及的技术并不限定于车载网络,也可以适用于机器人、产业设备等的网络等、车载网络之外的遵循CAN协议进行通信的网络通信系统。另外,CAN协议应该作为也包括自动化系统内的组装系统等所使用的CANOpen、或TTCAN(Time-Triggered CAN,时间触发CAN)、CANFD(CAN with Flexible Data Rate,灵活数据传输率的CAN)等的派生协议在内的广义上的含义的协议来对待。

[0243] (7) 在上述实施方式中,示出了不正常ECU连接于总线的例子,但也存在ECU400a~400d或ECU3400a~3400d这样的已有的ECU因某种原因而作为不正常ECU进行工作的可能性。即使在该情况下,通过如上述实施方式中示出的那样不正常检测ECU适当地检测不正常帧并发送错误帧,也能够阻止其他ECU处理不正常帧。

[0244] (8) 在实施方式2中,设为了使用对消息ID与所允许的数据范围进行了关联的数据范围列表,根据所接收到的数据帧的数据是否包含于按各个消息ID所允许的数据范围,进行是否不正常的判定,但也可以使数据范围列表不包含消息ID,预先确定对全部消息ID共同允许的数据范围(例如“0~180”),与消息ID无关地进行是否不正常的判定。另外,对于不

正常检测ECU所保持的数据范围列表,也可以设为对可能发送到连接有该不正常检测ECU的总线的消息ID与数据范围进行了关联的列表。由此,能够将数据范围列表也作为实施方式1中示出了的正规ID列表来使用。利用该数据范围列表在实施方式2所示的不正常检测ECU中也可以进行实施方式1中示出的消息ID的检查(时序S1004)。

[0245] (9)也可以取代实施方式2中示出的对消息ID与所允许的数据范围进行了关联的数据范围列表,设为不正常检测ECU使用对消息ID和所允许的数据长进行了关联的数据长度列表。该情况下,不正常检测ECU判定所接收到的数据帧的控制域的值是否符合表示不正常的预定条件。该表示不正常的预定条件是控制域中的数据长度(DLC)不是在数据长度列表中与消息ID关联的数据长度这一条件。不正常检测ECU根据所接收到的DCL是否为在数据长度列表中按各个消息ID所允许的数据长度,进行是否不正常的判定。

[0246] (10)在上述实施方式中,特别是着眼于数据帧进行了说明,但对于远程帧,不正常检测ECU也能够检测一定的不正常。例如,不正常检测ECU也可以使用实施方式1中示出的正规ID列表来判定所接收到的远程帧中的消息ID是否不正常。另外,不正常检测ECU也可以使用上述的数据长度列表,根据所接收到的远程帧中的控制域中的数据长度(DLC)是否为按各个消息ID所允许的数据长度来判定是否不正常。另外,对于上述实施方式中示出的通过不正常检测ECU接收到不正常帧而进行了不正常的检测的情况下所发送的错误帧,可以为在检测到不正常之后被迅速发送。此外,不正常检测ECU在检测到不正常之后、且该不正常帧的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者基于CRC检查的错误检测,将会中止该不正常帧的处理。此外,远程帧与数据帧同样地也包含消息ID、控制域以及CRC序列。

[0247] (11)在上述实施方式中,示出了不正常检测ECU在一定条件下发送示错消息,但也可以不发送示错消息。该情况下,网关以及头单元等的ECU不再需要特别保持与不正常检测ECU对应的结构(用于接收示错消息的接收ID列表等)。此外,不正常检测ECU也可以取代示错消息的发送而在自身具备扬声器或显示器等的情况下自己报告错误,还可以将出错的日志记录于存储介质等。

[0248] (12)上述实施方式中示出的不正常帧检测部以及不正常MAC检测部也可以安装于被称为CAN控制器的硬件、或在与CAN控制器连接并工作的处理器上进行工作的固件。另外,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也可以保存于被称为CAN控制器的硬件的寄存器、或在与CAN控制器连接并工作的处理器上进行工作的固件。

[0249] (13)上述实施方式中的各ECU(包括网关和头单元),例如是处理器、存储器等包括数字电路、模拟电路、通信线路等的装置,但也可以包括硬盘装置、显示器、键盘、鼠标等其他的硬件构成要素。另外,也可以取代由处理器执行存储器所存储的控制程序并以软件方式来实现功能,而通过专用的硬件(数字电路等)来实现其功能。

[0250] (14)上述实施方式中的构成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是将多个构成部集成于1个芯片上而制造出的超多功能LSI,具体而言,是包含微处理器、ROM、RAM等而构成的计算机系统。所述RAM中存储有计算机程序。所述微处理器按照所述计算机程序进行工作,由此系统LSI实现其功能。

[0251] 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。

[0252] 另外,虽然此处设为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FPGA (Field Programmable Gate Array;现场可编程门阵列) 或者可以对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)。

[0253] 进而,随着半导体技术的发展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。也可能存在应用生物技术的可能性。

[0254] (15) 构成上述各装置的构成要素的一部分或者全部也可以由能够装卸于各装置的IC卡或者单体模块构成。所述IC卡或者所述模块是由微处理器、ROM、RAM等构成的计算机系统。所述IC卡或者所述模块也可以包含上述超多功能LSI。微处理器按照计算机程序进行工作,由此所述IC卡或者所述模块实现其功能。该IC卡或者该模块也可以具有抗篡改性。

[0255] (16) 作为本公开的一个技术方案,也可以是上述所示的不正常应对方法等方法。另外,也可以是通过计算机实现这些方法的计算机程序,还可以是通过所述计算机程序形成的数字信号。

[0256] 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所述数字信号。

[0257] 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所述数字信号经由电通信线路、无线或有线通信线路、以因特网为代表的网络、数据广播等进行传输。

[0258] 另外,作为本公开的一个技术方案,也可以是具有微处理器和存储器的计算机系统,所述存储器记录有上述计算机程序,所述微处理器可以按照所述计算机程序进行工作。

[0259] 另外,也可以通过将所述程序或所述数字信号记录在所述记录介质中转移、或经由所述网络等将所述程序或所述数字信号进行转移,通过独立的其他的计算机系统来实施。

[0260] (17) 通过将上述实施方式以及上述变形例中示出的各构成要素以及功能进行任意组合而实现的实施方式也包含在本公开的范围中。

[0261] 产业上的可利用性

[0262] 本公开能够利用于在车载网络系统等中抑制不正常ECU的影响。

[0263] 附图标记的说明

[0264] 10、11、12 车载网络系统

[0265] 100a、100b、2100a、2100b、3100a、3100b 不正常检测电子控制单元(不正常检测ECU)

[0266] 110 不正常检测计数器保持部

[0267] 120 正规ID列表保持部

[0268] 130、2130 不正常帧检测部

- [0269] 140、230、320、420、3420 帧生成部
- [0270] 150、260、350、450、2150、3150 帧解释部
- [0271] 160、270、360、460 帧收发部
- [0272] 200 头单元
- [0273] 210 显示控制部
- [0274] 220、410 帧处理部
- [0275] 240、330、430 接收ID判断部
- [0276] 250、340、440 接收ID列表保持部
- [0277] 300 网关
- [0278] 310 传送处理部
- [0279] 370 传送规则保持部
- [0280] 400a、400b、400c、400d、3400a、3400b、3400c、3400d 电子控制单元 (ECU)
- [0281] 401 发动机
- [0282] 402 制动器
- [0283] 403 门开闭传感器
- [0284] 404 窗开闭传感器
- [0285] 470 数据取得部
- [0286] 500a、500b、500c 总线
- [0287] 2120 数据范围列表保持部
- [0288] 3130 不正常MAC检测部
- [0289] 3410、3170 MAC生成部
- [0290] 3430、3180 MAC密钥保持部
- [0291] 3440、3190 计数器保持部

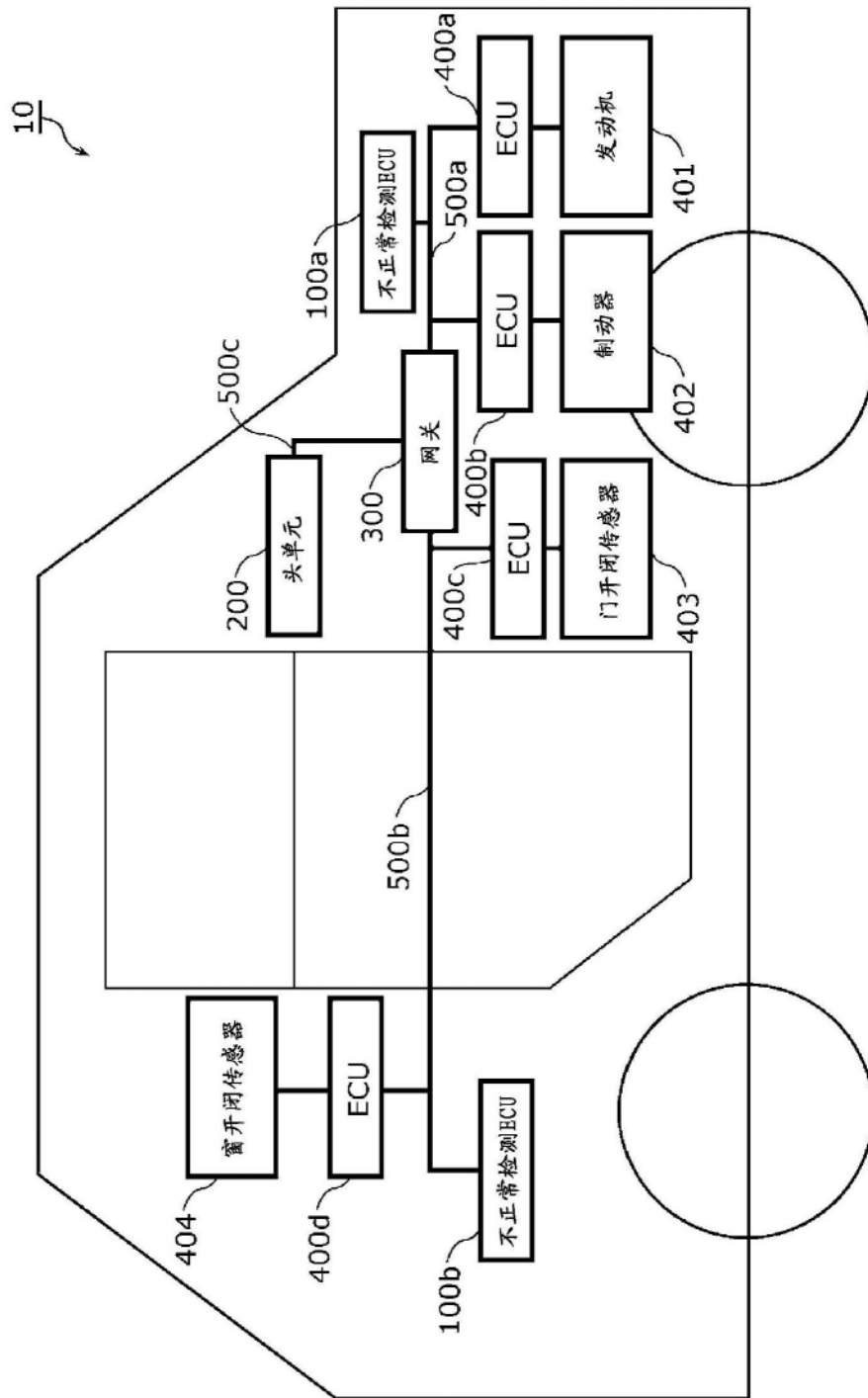


图1

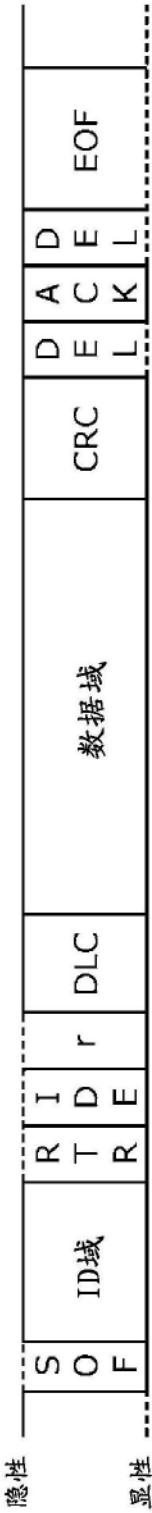


图2

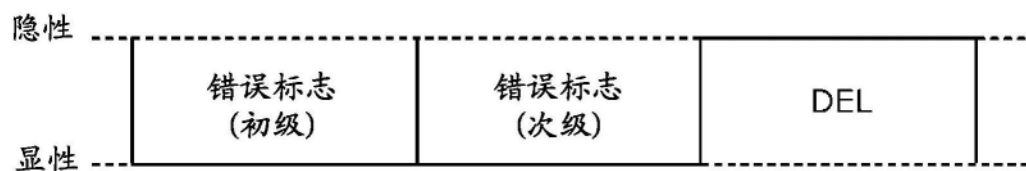


图3

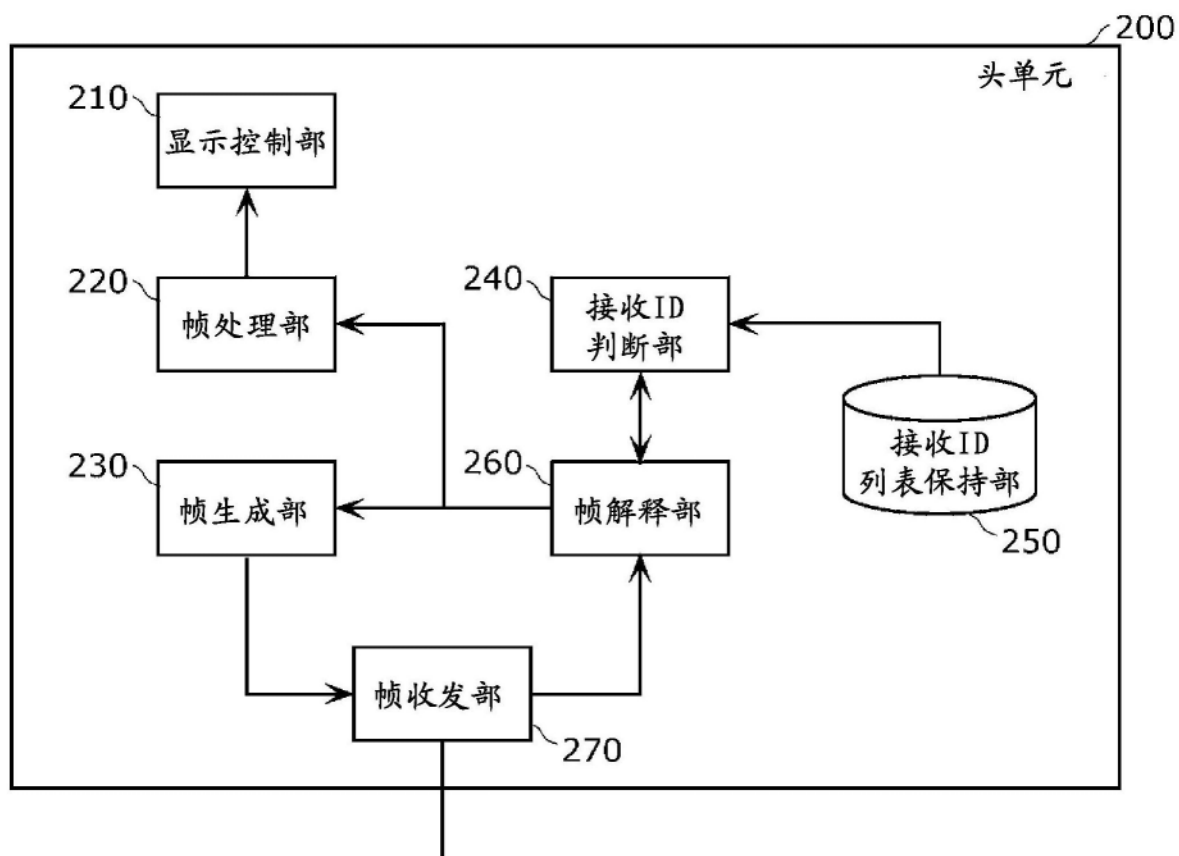


图4

接收ID列表
1
2
3
4

图5

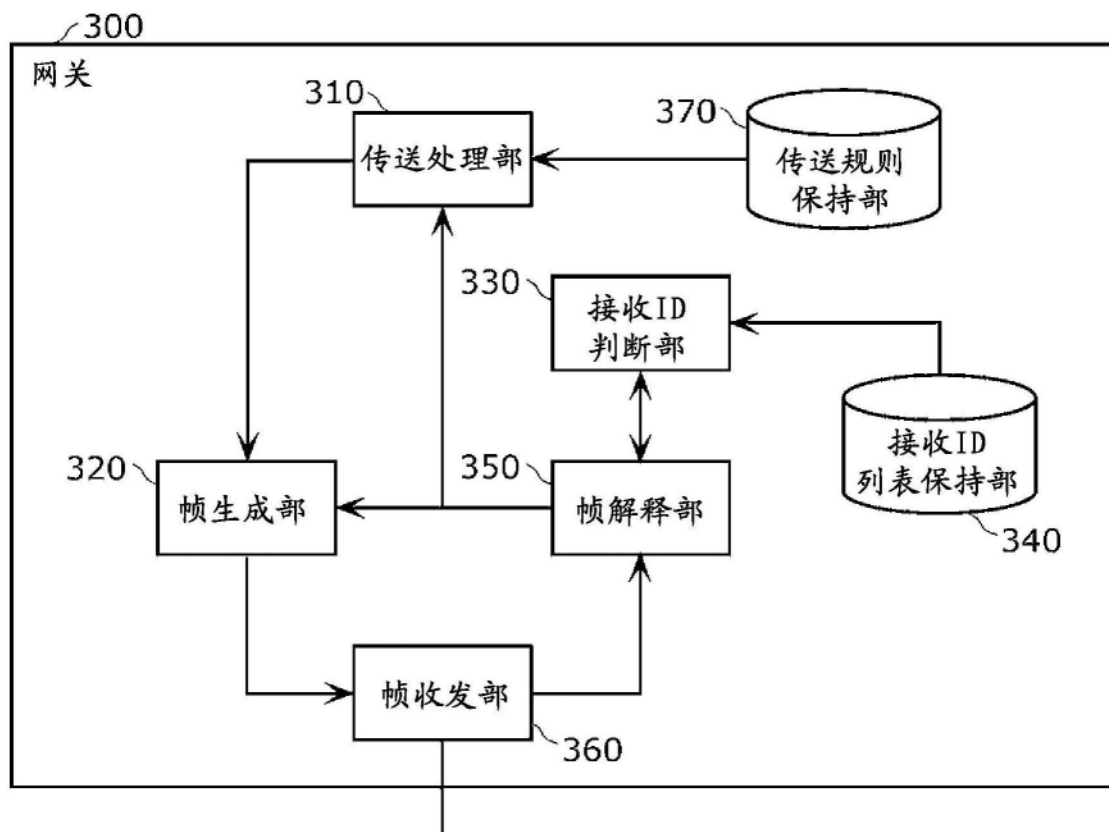


图6

传送规则

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

图7

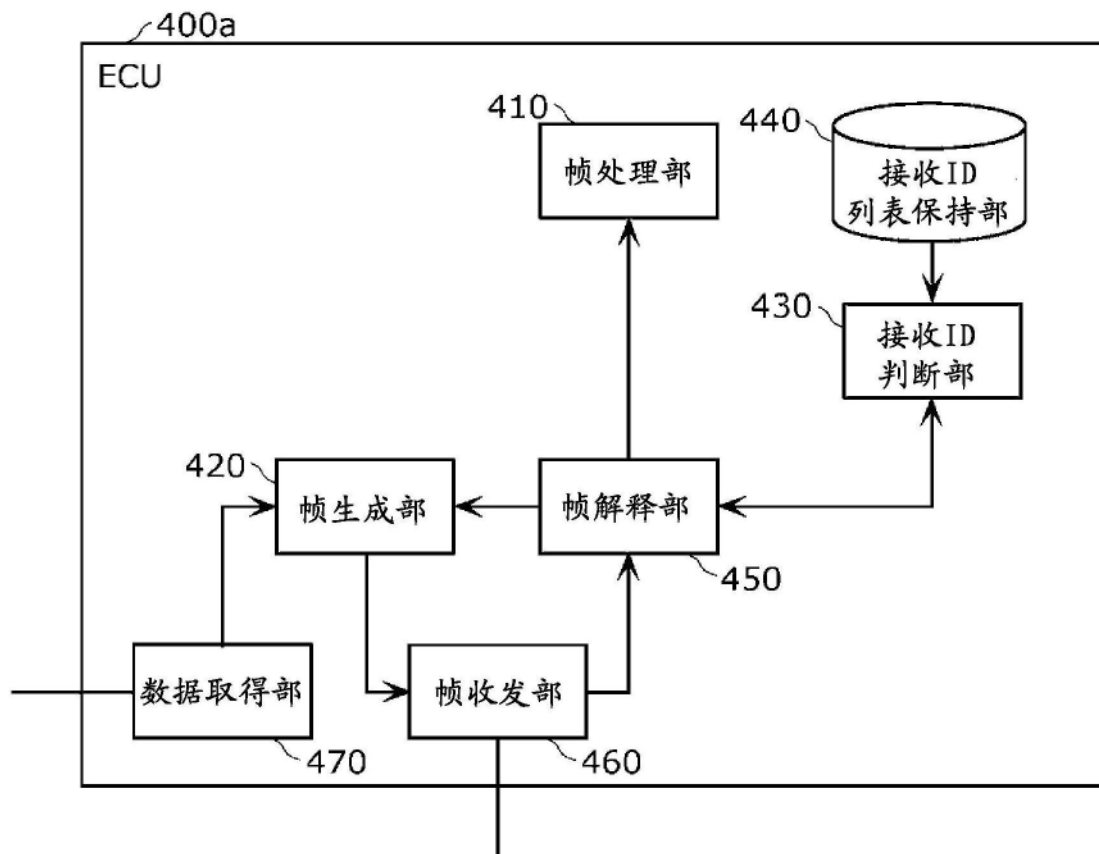


图8

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

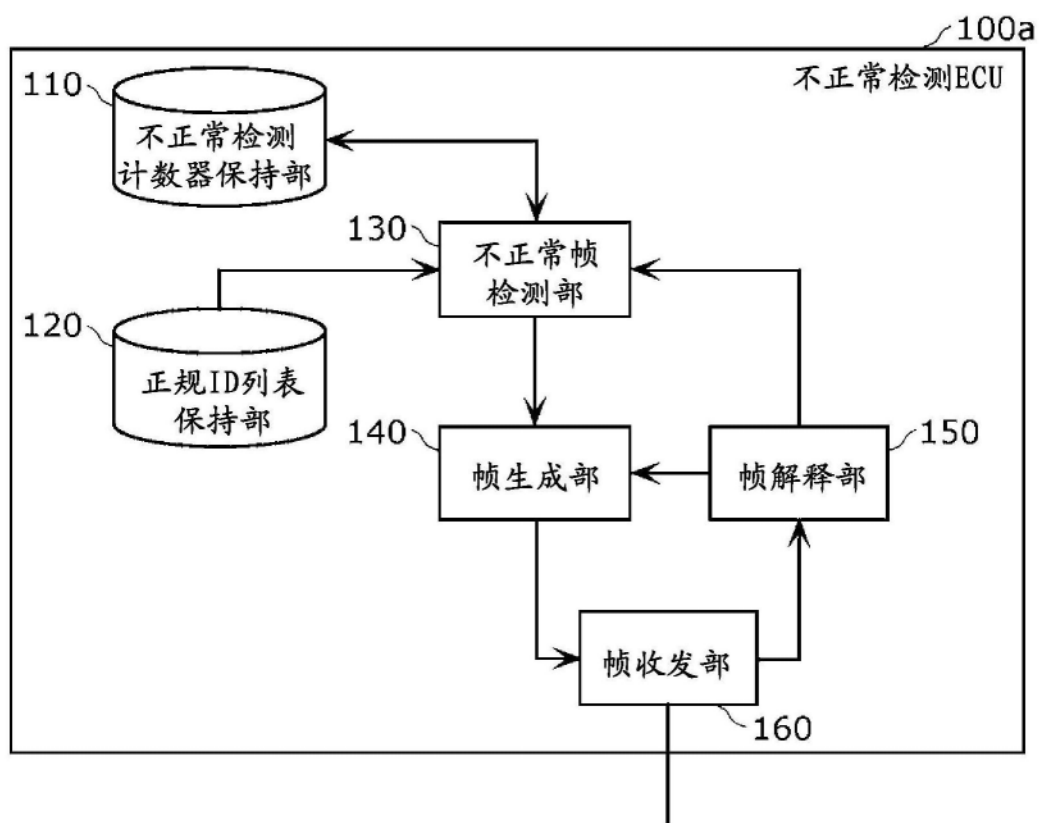


图14

正规ID列表
1
2
3

图15

正规ID列表
1
2
3
4

图16

ID	不正常检测计数器
1	0
2	0
3	0
4	1
5	0
...	...

图17

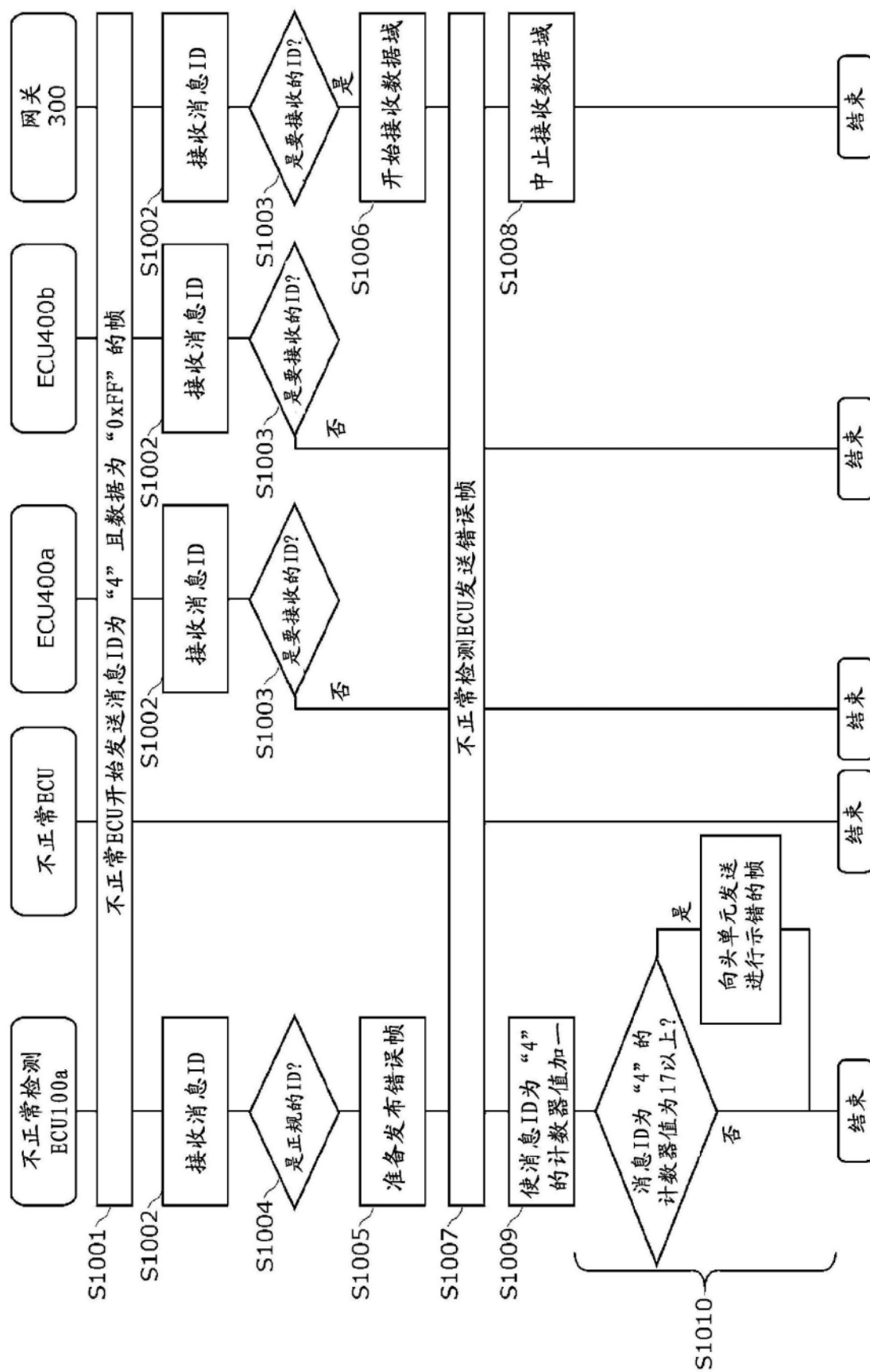


图18

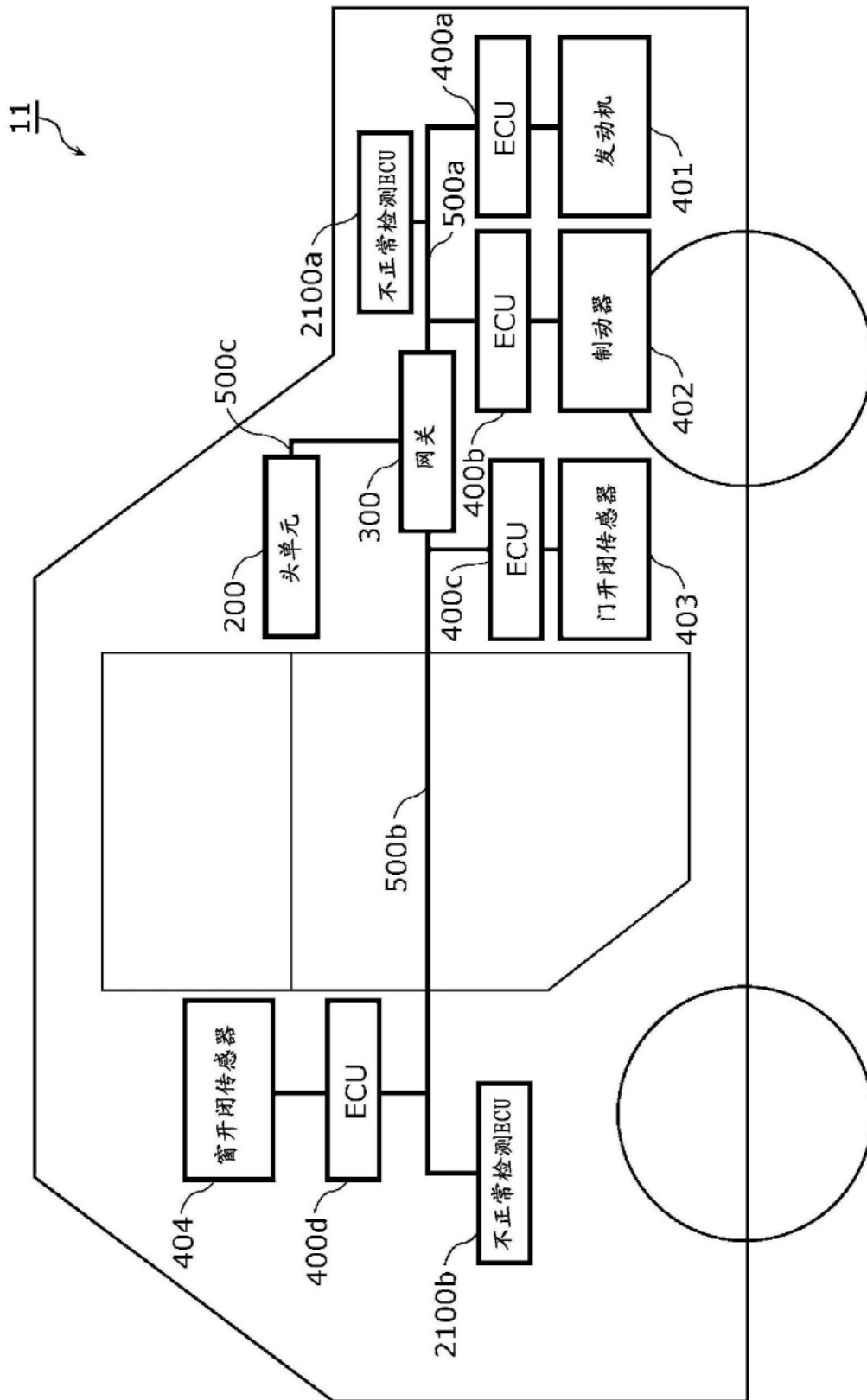


图19

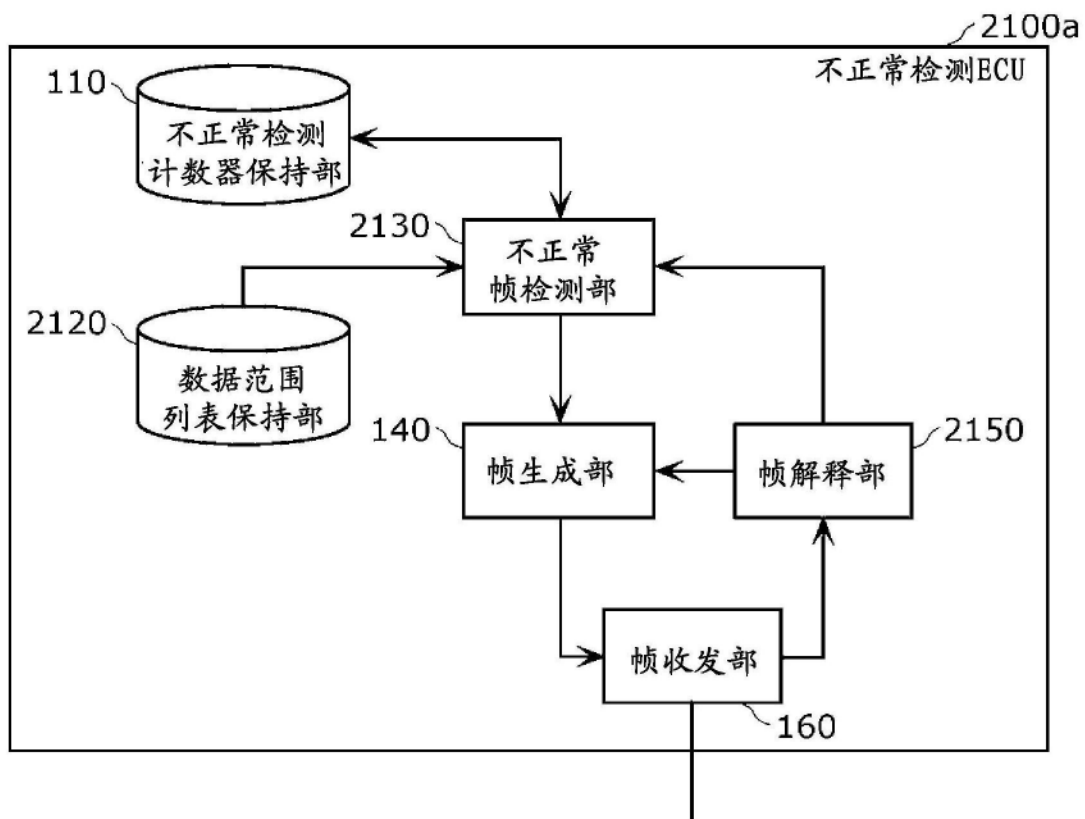


图20

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

图21

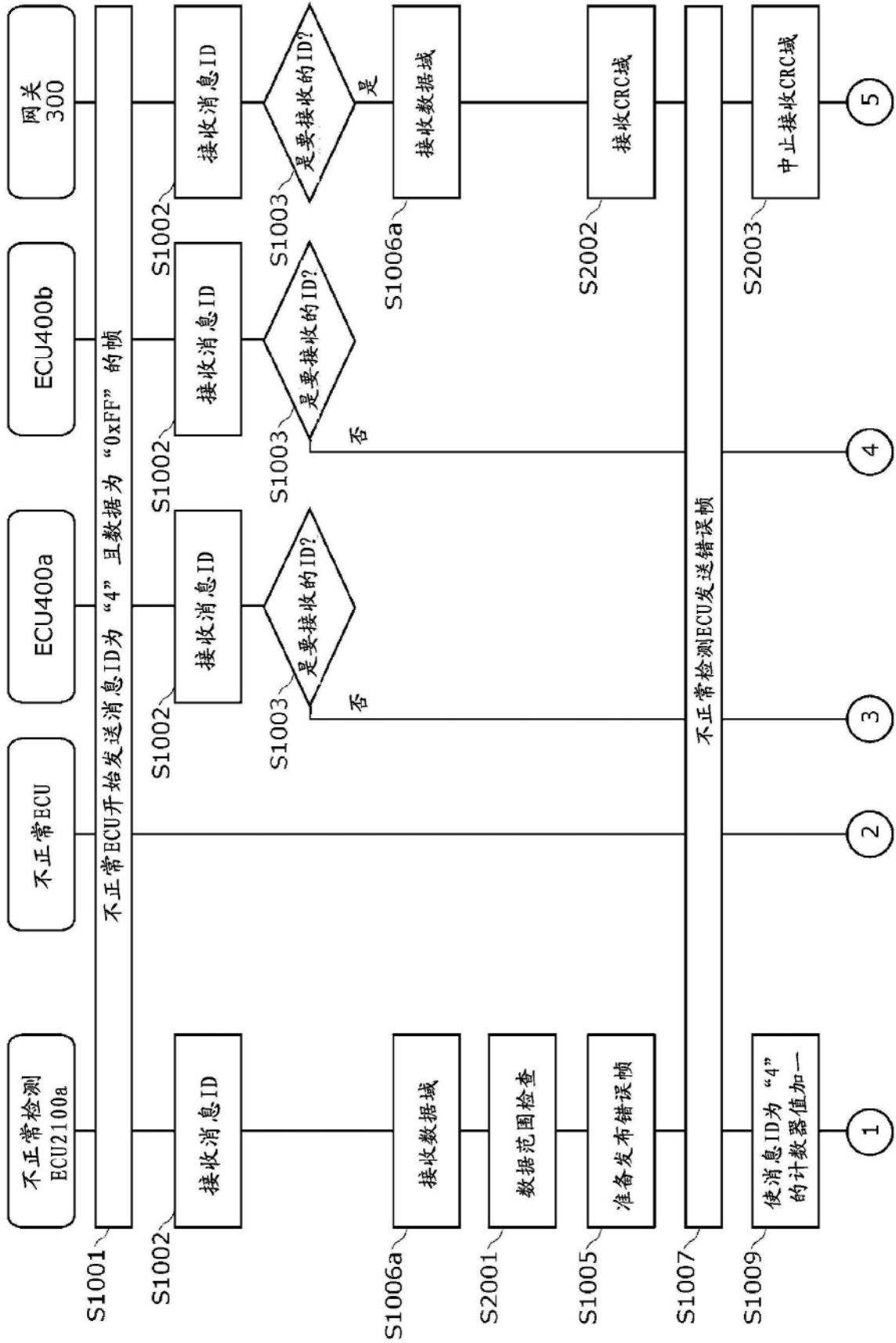


图22

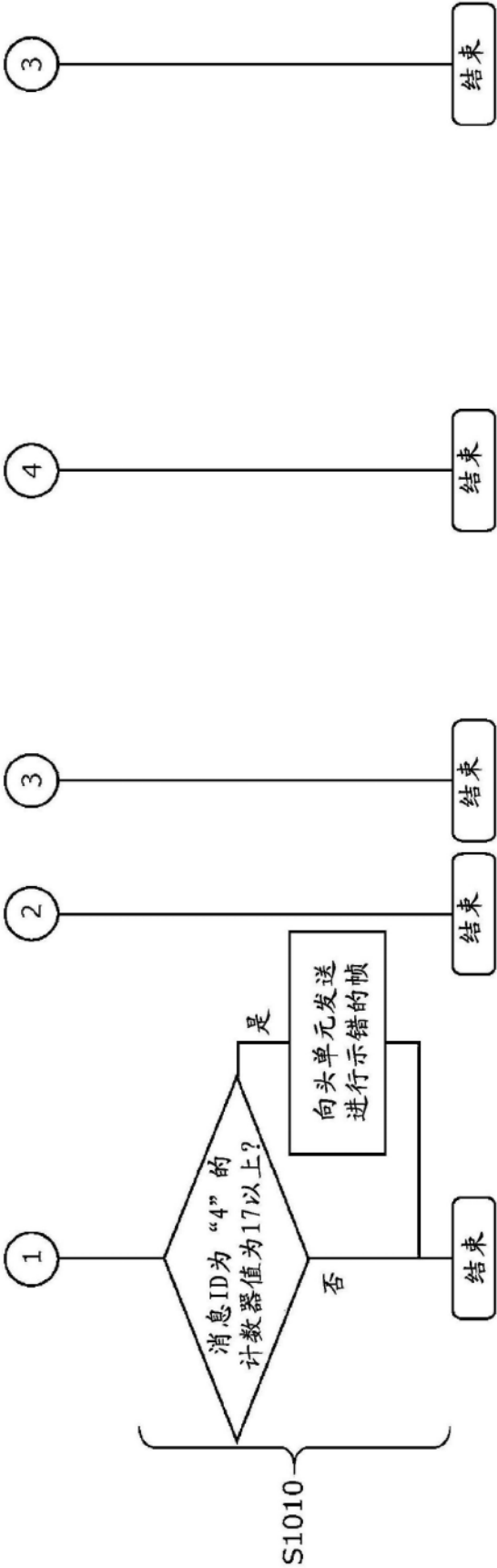


图23

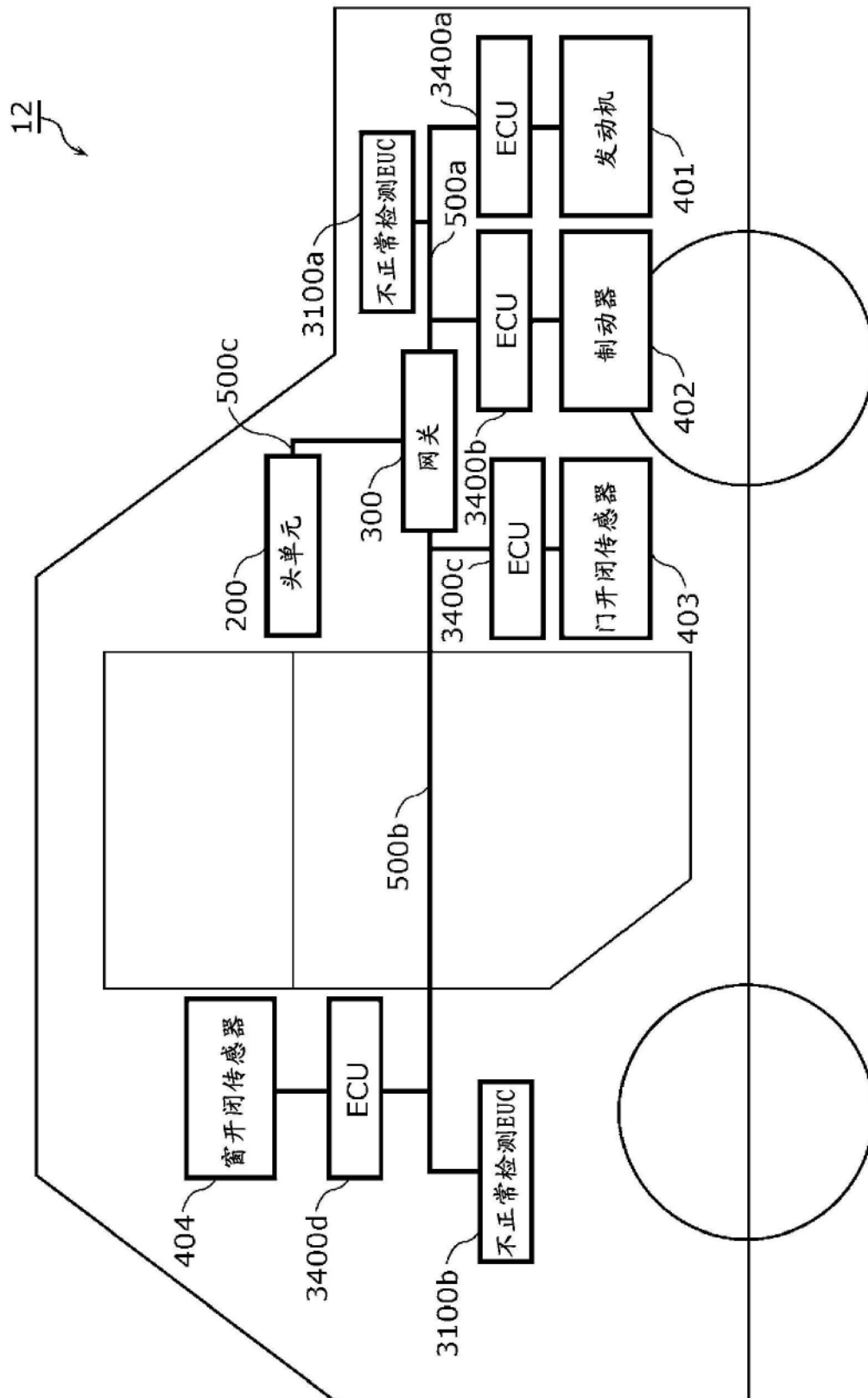


图24

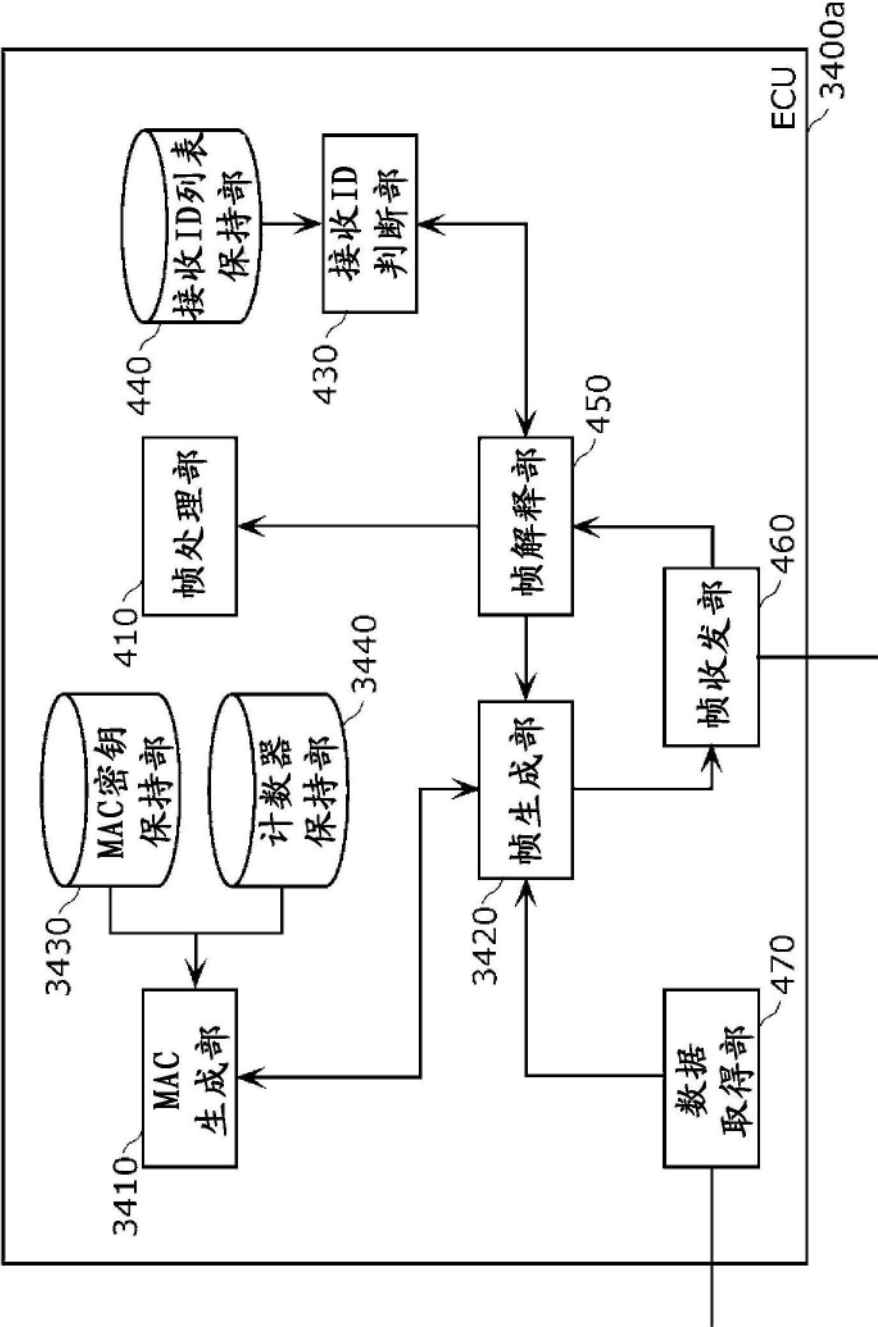


图25

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

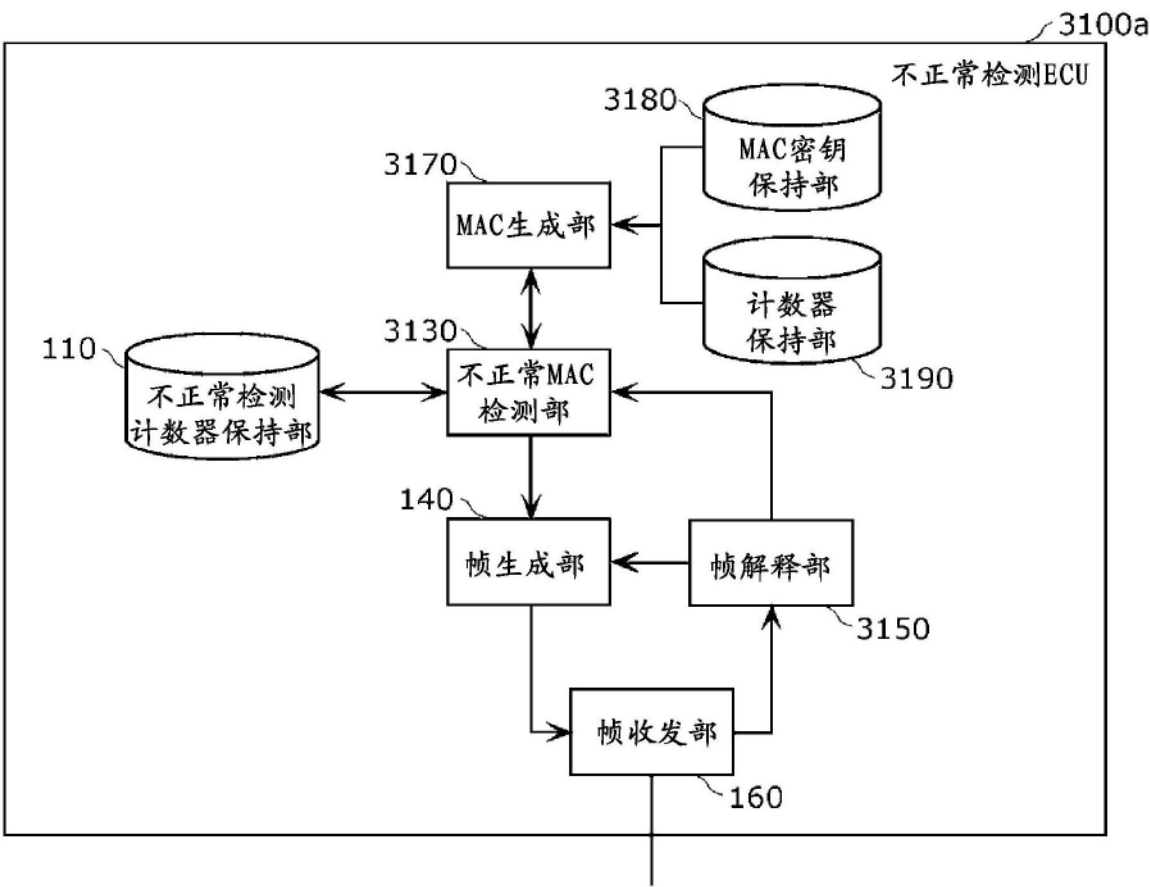


图30

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

图31

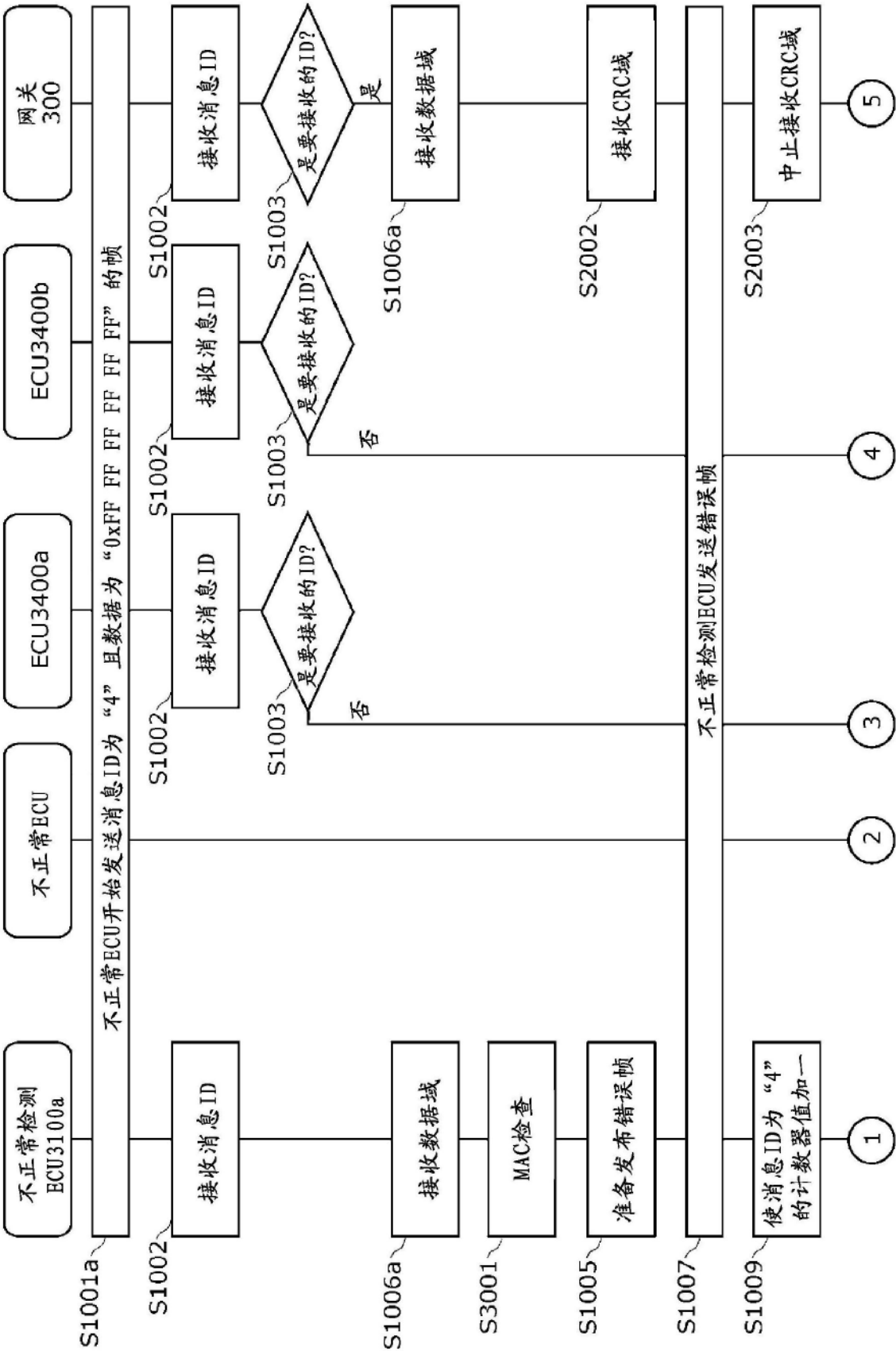


图32

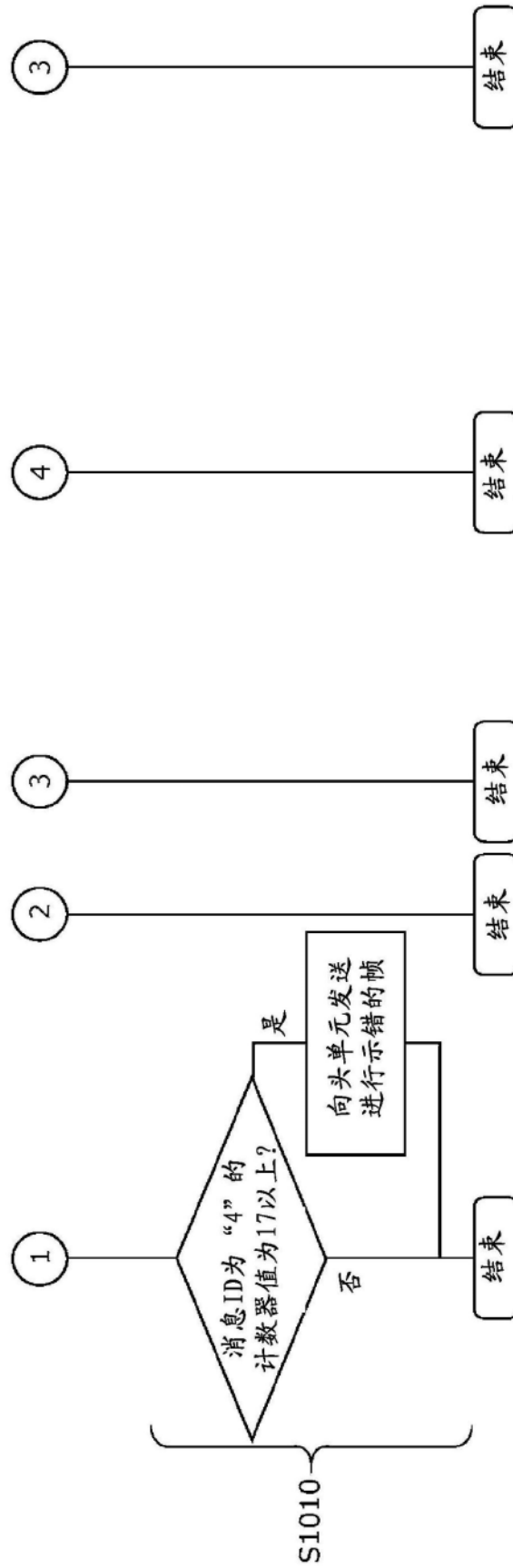


图33