



(12)发明专利

(10)授权公告号 CN 107113215 B

(45)授权公告日 2020.04.14

(21)申请号 201680004971.0

(22)申请日 2016.01.13

(65)同一申请的已公布的文献号  
申请公布号 CN 107113215 A

(43)申请公布日 2017.08.29

(30)优先权数据  
2015-005260 2015.01.14 JP

(85)PCT国际申请进入国家阶段日  
2017.07.04

(86)PCT国际申请的申请数据  
PCT/JP2016/050826 2016.01.13

(87)PCT国际申请的公布数据  
W02016/114301 JA 2016.07.21

(73)专利权人 国立大学法人名古屋大学  
地址 日本爱知县  
专利权人 株式会社自动网络技术研究所

住友电装株式会社  
住友电气工业株式会社

(72)发明人 高田广章 仓地亮 上田浩史

(74)专利代理机构 中原信达知识产权代理有限  
责任公司 11219  
代理人 赵晶 高培培

(51)Int.Cl.  
H04L 12/40(2006.01)  
H04L 12/28(2006.01)

(56)对比文件  
JP 2009181431 A,2009.08.13,  
US 2008043830 A1,2008.02.21,  
JP 2005333222 A,2005.12.02,  
US 2014380416 A1,2014.12.25,

审查员 高修会

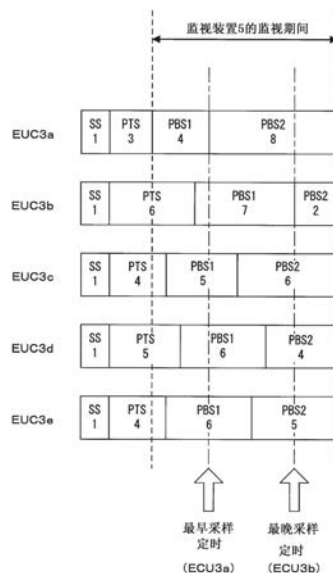
权利要求书1页 说明书9页 附图8页

(54)发明名称

通信系统、异常检测装置及异常检测方法

(57)摘要

提供一种能够检测利用了多个通信装置的采样定时的差异的信息篡改等与通信相关的异常的通信系统、异常检测装置及异常检测方法。对于ECU(3a~3e)经由共用的通信线进行信息的发送接收的系统结构,利用与该通信线连接的监视装置进行与通信相关的异常检测。各ECU(3a~3b)在一比特的信息的发送期间中以规定的定时进行一次采样,由此来接收信息。但是,容许多个ECU(3a~3e)以不同的定时进行采样的情况。监视装置在一比特的信息的发送期间,在包含基于ECU(3a~3e)的最早的采样的定时和最晚的采样的定时的规定的监视期间,对通信线的电压进行多次采样,基于多次的采样的结果进行异常检测。



1. 一种通信系统,具备经由共用的通信线而连接并经由该通信线进行二值的信息的发送接收的多个通信装置,所述通信装置分别具有接收部,该接收部在一比特的信息的发送期间中以规定的定时对所述通信线的电压进行一次采样,由此进行信息的接收,所述通信系统容许所述多个通信装置以不同的定时进行采样的情况,所述通信系统的特征在于,

所述通信系统具备异常检测装置,

所述异常检测装置与所述通信线连接,

所述异常检测装置具有:

采样部,在包含由所述多个通信装置进行的采样中的最早的采样的定时及最晚的采样的定时的规定期间,对所述通信线的电压进行多次采样;及

检测部,基于该采样部的多个采样结果来检测与通信相关的异常。

2. 根据权利要求1所述的通信系统,其特征在于,

所述采样部在所述规定期间周期性地多次采样,

在所述采样部采样的采样结果与以前的采样结果不同的情况下,所述检测部检测到与通信相关的异常。

3. 根据权利要求1或权利要求2所述的通信系统,其特征在于,

所述异常检测装置具有通知部,该通知部在所述检测部检测到异常的情况下向所述多个通信装置通知检测到异常。

4. 根据权利要求3所述的通信系统,其特征在于,

在所述检测部检测到异常的情况下,所述通知部进行对于所述通信线的规定的信息发送,

利用该信息发送来阻碍由所述多个通信装置进行的信息的接收。

5. 一种异常检测装置,在通信系统中检测与通信相关的异常,所述通信系统具备经由共用的通信线而连接并经由该通信线进行二值的信息的发送接收的多个通信装置,所述通信装置分别具有接收部,该接收部在一比特的信息的发送期间中以规定的定时对所述通信线的电压进行一次采样,由此进行信息的接收,所述通信系统容许所述多个通信装置以不同的定时进行采样的情况,所述异常检测装置的特征在于,

所述异常检测装置与所述通信线连接,

所述异常检测装置具有:

采样部,在包含由所述多个通信装置进行的采样中的最早的采样的定时及最晚的采样的定时的规定期间,对所述通信线的电压进行多次采样;及

检测部,基于该采样部的多个采样结果来检测与通信相关的异常。

6. 一种异常检测方法,在通信系统中检测通信的异常,所述通信系统具备经由共用的通信线而连接并经由该通信线进行二值的信息的发送接收的多个通信装置,所述通信装置分别具有接收部,该接收部在一比特的信息的发送期间中以规定的定时对所述通信线的电压进行一次采样,由此进行信息的接收,所述通信系统容许所述多个通信装置以不同的定时进行采样的情况,所述异常检测方法的特征在于,

在包含由所述多个通信装置进行的采样中的最早的采样的定时及最晚的采样的定时的规定期间,对所述通信线的电压进行多次采样,

基于多次的采样结果来检测与通信相关的异常。

## 通信系统、异常检测装置及异常检测方法

### 技术领域

[0001] 涉及一种在多个通信装置连接于共用的通信线的结构中能够检测与通信相关的异常的通信系统、异常检测装置及异常检测方法。

### 背景技术

[0002] 以往,搭载于车辆的多个ECU(Electronic Control Unit:电子控制单元)间的通信广泛地采用CAN的通信协议。采用了CAN的通信协议的通信系统成为多个ECU连接于共用的CAN总线的结构,接收侧的ECU对于发送侧的ECU向CAN总线输出的信号进行采样,由此进行信息的发送接收。而且,发送侧的ECU进行向CAN总线的信号输出,并对CAN总线的信号进行采样,由此来检测与自身发送的信息相关的变化的有无。

[0003] 在非专利文献1中,指出了如下情况:在发送侧的ECU和接收侧的ECU中对CAN总线的信号进行采样的定时不同的情况下,通过仅在接收侧的ECU进行采样的短期间内有意地使CAN总线上的信号变化,发送侧的ECU不会察觉,接收侧的ECU有可能接收篡改了的信息。

[0004] 在先技术文献

[0005] 非专利文献

[0006] 非专利文献1:松本勉、向达泰希、土屋游、中山淑文、吉冈克成,“对于电气性的数据篡改的CAN的完整强化对策”,计算机安全论文集2014,2014年10月22日~24日

### 发明内容

[0007] 发明要解决的课题

[0008] 例如对于配置在车辆内的CAN总线连接不正当的设备,通过非专利文献1记载的方法进行了对于特定的ECU的信息篡改的情况下,在搭载于车辆的各种电子设备中可能会发生误动作等。由此,要求检测或防止这样的信息篡改的技术。

[0009] 本发明鉴于这样的情况而作出,其目的在于提供一种能够检测利用了多个通信装置的采样定时的差异的信息篡改等与通信相关的异常的通信系统、异常检测装置及异常检测方法。

[0010] 用于解决课题的方案

[0011] 本发明的通信系统具备经由共用的通信线而连接并经由该通信线进行二值的信息的发送接收的多个通信装置,所述通信装置分别具有接收部,该接收部在一比特的信息的发送期间中以规定的定时对所述通信线的电压进行一次采样,由此进行信息的接收,所述通信系统容许所述多个通信装置以不同的定时进行采样的情况,所述通信系统的特征在于,所述通信系统具备异常检测装置,所述异常检测装置与所述通信线连接,所述异常检测装置具有:采样部,在包含由所述多个通信装置进行的采样中的最早的采样的定时及最晚的采样的定时的规定期间,对所述通信线的电压进行多次采样;及检测部,基于该采样部的多个采样结果来检测与通信相关的异常。

[0012] 另外,本发明的通信系统的特征在于,所述采样部在所述规定期间周期性地

多次采样,在所述采样部采样的采样结果与以前的采样结果不同的情况下,所述检测部检测到与通信相关的异常。

[0013] 另外,本发明的通信系统的特征在于,所述异常检测装置具有通知部,该通知部在所述检测部检测到异常的情况下向所述多个通信装置通知检测到异常。

[0014] 另外,本发明的通信系统的特征在于,在所述检测部检测到异常的情况下,所述通知部进行对于所述通信线的规定的信息发送,利用该信息发送来阻碍由所述多个通信装置进行的信息接收。

[0015] 另外,本发明的异常检测装置在通信系统中检测与通信相关的异常,所述通信系统具备经由共用的通信线而连接并经由该通信线进行二值的信息的发送接收的多个通信装置,所述通信装置分别具有接收部,该接收部在一比特的信息的发送期间中以规定的定时对所述通信线的电压进行一次采样,由此进行信息的接收,所述通信系统容许所述多个通信装置以不同的定时进行采样的情况,所述异常检测装置的特征在于,所述异常检测装置与所述通信线连接,所述异常检测装置具有:采样部,在包含由所述多个通信装置进行的采样中的最早的采样的定时及最晚的采样的定时的规定期间,对所述通信线的电压进行多次采样;及检测部,基于该采样部的多个采样结果来检测与通信相关的异常。

[0016] 另外,本发明的异常检测方法在通信系统中检测通信的异常,所述通信系统具备经由共用的通信线而连接并经由该通信线进行二值的信息的发送接收的多个通信装置,所述通信装置分别具有接收部,该接收部在一比特的信息的发送期间中以规定的定时对所述通信线的电压进行一次采样,由此进行信息的接收,所述通信系统容许所述多个通信装置以不同的定时进行采样的情况,所述异常检测方法的特征在于,在包含由所述多个通信装置进行的采样中的最早的采样的定时及最晚的采样的定时的规定期间,对所述通信线的电压进行多次采样,基于多次的采样结果来检测与通信相关的异常。

[0017] 在本发明的通信系统中,对于多个通信装置经由共用的通信线进行信息的发送接收的系统结构,利用与该通信线连接的异常检测装置进行与通信相关的异常检测。各通信装置在一比特的信息的发送期间中以规定的定时进行一次的采样,由此接收信息。但是,容许多个通信装置以不同的定时进行采样的情况。异常检测装置在一比特的信息的发送期间中,在包含由通信装置进行的最早的采样的定时和最晚的采样的定时的规定期间,对通信线的电压进行多次采样。异常检测装置在通信系统所包含的多个通信装置可进行采样的期间,能够监视共用的通信线的电压的变化等,能够基于多次的采样的结果进行异常检测。

[0018] 另外,在本发明中,异常检测装置在规定期间周期性地多次采样,在本次的采样结果与以前的采样结果不同的情况下,即在规定的期间中通信线的信号发生了变化的情况下,判断为通信发生了异常。由此,能够检测对应于特定的通信装置的采样定时而使信号变化所引起的信息篡改。

[0019] 另外,在本发明中,在检测到与通信相关的异常的情况下,异常检测装置向多个通信装置进行通知。异常检测装置例如将CAN协议的错误帧对于通信线输出等,通过进行规定的信息发送而能够通知异常的发生。而且,在本通信系统中,通过基于异常检测装置的异常通知用的信息发送,在通信系统中的各通信装置中阻碍信息的接收。由此,能够防止篡改后的信息被通信装置接收的情况。

[0020] 发明效果

[0021] 在本发明的情况下,异常检测装置能够检测利用了每个通信装置的采样定时的差异的信息篡改等的与通信相关的异常。

### 附图说明

[0022] 图1是表示本实施方式的通信系统的结构的示意图。

[0023] 图2是表示ECU的结构框图。

[0024] 图3是表示监视装置的结构框图。

[0025] 图4是用于说明监视装置的监视期间的示意图。

[0026] 图5是用于说明监视装置的监视处理的状态转换图。

[0027] 图6是表示监视装置在同步状态下进行的处理的次序的流程图。

[0028] 图7是表示监视装置在第一监视状态下进行的处理的次序的流程图。

[0029] 图8是表示监视装置在第二监视状态下进行的处理的次序的流程图。

### 具体实施方式

[0030] 以下,基于表示本发明的实施方式的附图而具体地说明本发明。

[0031] <系统结构>

[0032] 图1是表示本实施方式的通信系统的结构的示意图。本实施方式的通信系统具备搭载于车辆1的多个ECU3、及一个监视装置5而构成。ECU3及监视装置5经由铺设于车辆1的共用的通信线而连接,能够相互发送接收消息。在本实施方式中,将该通信线设为CAN总线,ECU3及监视装置5进行遵照CAN协议的通信。ECU3可以是例如进行车辆1的发动机的控制的发动机ECU、进行车身的电气安装件的控制的车身ECU、进行与ABS(Antilock Brake System:防抱制动系统)相关的控制的ABS-ECU、或者进行车辆1的气囊的控制的气囊ECU等那样的各种电子控制装置。监视装置5是监视对于车内网络的不正当的消息发送的装置。监视装置5可以设置作为监视专用的装置,也可以是例如向网关等装置附加了监视的功能的结构,而且还可以是例如向任一个ECU3附加了监视的功能的结构。

[0033] 图2是表示ECU3的结构框图。需要说明的是,在图2中,关于在车辆1设置的多个ECU3,抽出并图示与通信相关的块,各ECU3特有的与车辆控制等相关的块省略图示。图2图示的这些块是多个ECU3共用而设置的块。本实施方式的ECU3具备处理部31、ROM(Read Only Memory)32、RAM(Random Access Memory)33及CAN通信部34等而构成。处理部31使用CPU(Central Processing Unit:中央处理单元)或MPU(Micro-Processing Unit:微处理单元)等运算处理装置而构成。处理部31读出存储于ROM32的程序并执行,由此进行车辆1的各种信息处理或控制处理等。

[0034] ROM32使用闪存或EEPROM(Electrically Erasable Programmable ROM:电可擦可编程程序只读存储器)等非易失性的存储器元件而构成。ROM32存储有处理部31执行的程序和由此进行的处理所需的各种数据。需要说明的是,存储于ROM32的程序及数据对于每个ECU3不同。RAM33使用SRAM(Static Random Access Memory:静态随机存取存储器)或DRAM(Dynamic Random Access Memory:动态随机存取存储器)等的能够进行数据改写的存储器元件而构成。RAM33存储通过处理部31的处理而生成各种数据。

[0035] CAN通信部34遵照CAN的通信协议,进行经由CAN总线的与其他的ECU3或监视装置5

的通信。CAN通信部34具有发送部35,该发送部35将从处理部31提供的发送用的信息转换成遵照CAN的通信协议的信号,并将变换后的信号向CAN总线输出,由此进行向其他的ECU3或监视装置5的信息发送。而且,CAN通信部34具有接收部36,该接收部36通过对CAN总线的电位进行采样,而取得其他的ECU3或监视装置5输出的信号,并将该信号遵照CAN的通信协议转换成二值的信息,由此进行信息的接收。接收部36将接收到的信息向处理部31提供。

[0036] 另外,CAN通信部34在自身的消息发送与其他的ECU3或监视装置5的消息发送发生冲突的情况下,进行调解先发送哪个消息的处理,所谓仲裁处理。在各ECU3发送的消息中,根据消息的类别而预先确定ID。该ID是作为数值而处理的信息,该值越小,则消息发送的优先度越高。因此,在通信系统中,在CAN总线上多个消息发送发生冲突的情况下,进行优先度最高的消息的发送,在该消息的发送完成后进行其他的消息的发送。需要说明的是,CAN通信部34进行的仲裁处理是现存的技术,因此省略详细的处理次序的说明。

[0037] 图3是表示监视装置5的结构框图。监视装置5具备处理部51、存储部52及CAN通信部53等而构成。处理部51使用CPU或MPU等运算处理装置而构成,读出存储于存储部52的程序并执行,由此进行监视车辆1的ECU3的行为及通信等的处理。存储部52使用闪存或EEPROM等的能够进行数据改写的非易失性的存储器元件而构成。在本实施方式中,存储部52将与在通信系统所包含的各ECU3接收消息时对CAN总线上的信号进行采样的定时相关的信息存储作为定时信息52a。

[0038] CAN通信部53遵照CAN的通信协议,进行经由CAN总线的与ECU3的通信。CAN通信部53具有发送部54,该发送部54将从处理部51提供的发送用的信息转换成遵照CAN的通信协议的信号,并将变换后的信号向CAN总线输出,由此进行向ECU3的信息发送。而且,CAN通信部53具有接收部55,该接收部55通过对CAN总线的电位进行采样,来取得ECU3输出的信号,并将该信号遵照CAN的通信协议而转换成二值的信息,由此进行信息的接收。接收部55将接收到的信息向处理部51提供。

[0039] 另外,本实施方式的监视装置5的CAN通信部53还具有采样部56及异常检测部57作为通信系统的通信异常的检测的功能块。采样部56在通信系统中经由CAN总线发送接收的消息的一比特的发送期间中,进行多次CAN总线上的信号的采样。需要说明的是,在以往的遵照CAN协议进行通信的ECU3中,在消息的一比特期间中进行一次采样,通过该采样结果进行消息接收。在本实施方式的通信系统中,监视装置5在一比特期间中进行多次采样,由此能够取得一比特期间中的信号的变化而进行异常检测。

[0040] CAN通信部53的异常检测部57基于采样部56进行的多次的采样结果,进行检测通信系统中的通信的异常的处理。在本实施方式中,异常检测部57在采样部56每次进行采样时取得其结果,并判定上次的采样结果与本次的采样结果是否一致。在两采样结果一致的情况下,异常检测部57判断为未发生异常,继续进行采样结果的取得及比较。相对于此,在两采样结果不一致的情况下,异常检测部57判断为通信发生了异常,并向处理部51通知。

[0041] 在本实施方式中,在监视装置5的处理部51设有异常通知处理部61。异常通知处理部61可以是构成作为硬件的功能块的结构,也可以是构成作为软件的功能块的结构。异常通知处理部61在从CAN通信部53的异常检测部57提供了通信检测到异常的内容的通知时,进行向通信系统所包含的各ECU3通知异常发生的处理。在本实施方式中,异常通知处理部61使CAN通信部53向CAN总线输出错误帧,从而进行向ECU3的异常发生的通知。由此,通信发生

了异常时发送的消息(数据帧等)因监视装置5的错误帧而发送受到阻碍。接收到错误帧的各ECU3将这以前进行了接收处理的消息废弃。由此,能够防止有可能包含异常的消息被ECU3接收的情况。

[0042] <监视处理>

[0043] 在本实施方式的通信系统中,关于ECU3对CAN总线输出的消息,监视装置5监视异常的有无。需要说明的是,监视装置5的监视可以例如始终进行,而且也可以例如对于附有特定的ID的消息发送来进行。在本实施方式中,监视装置5始终进行监视。

[0044] 在本通信系统中发送接收的消息是显性(0)/隐性(1)的二值的数字数据遍及多个比特相连的消息,是所谓CAN协议的数据帧等。在通信系统中,预先确定对消息中所包含的一比特的数据进行发送的期间。监视装置5在一比特的发送期间中,在比该发送期间短的规定的监视期间,研究该一比特的数据是否发生了变化,由此来监视通信异常。

[0045] 图4是用于说明基于监视装置5的监视期间的示意图。CAN协议中的消息的一比特由4个期间(段)构成。即,CAN协议的一比特由SS(同步段)、PTS(传播时间段)、PBS1(相位缓冲段1)及PBS2(相位缓冲段2)这4个段构成。各段的长度(时间)决定作为基准时间 $T_q$ (Time Quantum)的整数倍。基准时间 $T_q$ 是各ECU3的CAN通信部34生成的采样用的时钟信号的周期。需要说明的是,SS的长度确定为 $1T_q$ 。PTS、PBS1及PBS2的长度可以对于每个ECU3设定不同的值。

[0046] SS是各ECU3用于进行同步的段,可期待信号的边缘处于该段之中的情况。PTS是用于吸收CAN总线上的信号延迟及杂音等的影响的段。PTS可以在 $1T_q \sim 8T_q$ 的范围内设定。PBS1是信号的边缘未进入SS之中时的用于保证误差的段。PBS1可以在 $1T_q \sim 8T_q$ 的范围内设定,能延长或缩短SJW(同步跳跃幅度)的时间。PBS2是在迅速检测到信号的边缘的情况下缩短SJW的时间的段。PBS2可以在 $2T_q \sim 8T_q$ 的范围内设定。需要说明的是,各ECU3的CAN通信部34进行采样的定时是从PBS1向PBS2转移的定时。

[0047] 例如在图4中,本实施方式的通信系统包含5个ECU3(以下,区别记载作为ECU3a~3e),示出各ECU3a~3e的段结构。ECU3a中,SS为 $1T_q$ ,PTS为 $3T_q$ ,PBS1为 $4T_q$ ,PBS2为 $8T_q$ 。ECU3b中,SS为 $1T_q$ ,PTS为 $6T_q$ ,PBS1为 $7T_q$ ,PBS2为 $2T_q$ 。ECU3c中,SS为 $1T_q$ ,PTS为 $4T_q$ ,PBS1为 $5T_q$ ,PBS2为 $6T_q$ 。ECU3d中,SS为 $1T_q$ ,PTS为 $5T_q$ ,PBS1为 $6T_q$ ,PBS2为 $4T_q$ 。ECU3e中,SS为 $1T_q$ ,PTS为 $4T_q$ ,PBS1为 $6T_q$ ,PBS2为 $5T_q$ 。需要说明的是,这些段的长度是一例,并不局限于此。

[0048] 本实施方式的监视装置5将监视的通信系统所包含的与各ECU3a~3e的段结构相关的信息作为定时信息52a而存储于存储部52。监视装置5的CAN通信部53基于存储于存储部52的定时信息52a,来决定进行通信异常的监视的监视期间。基于各ECU3a~3e的CAN通信部34的采样定时是从PBS1向PBS2转移的定时。由此,在本例中,最早进行基于ECU3a的采样,最晚进行基于ECU3b的采样。监视装置5的CAN通信部53以包含最早的采样定时和最晚的采样定时的方式决定监视期间。需要说明的是,在本实施方式中,将使设定有最早的采样定时的ECU3a的PBS1及PBS2相加而得到的期间作为基于监视装置5的CAN通信部53的监视期间。需要说明的是,在因某些理由而PBS1或PBS2的期间延长或缩短的情况下,该监视期间与之相伴地延长或缩短。

[0049] 在进行了基于ECU3的消息发送的情况下,监视装置5的CAN通信部53关于消息的各比特来进行监视期间的监视。CAN通信部53的采样部56在监视期间中以每 $1T_q$ 一次的频度,

对CAN总线上的信号进行采样。在图4所示的例子中,监视期间是PBS1的4T<sub>q</sub>+PBS2的8T<sub>q</sub>,因此采样部56在监视期间中总计进行12次的采样。采样部56的采样结果向异常检测部57提供。

[0050] 异常检测部57从监视期间中的取得了采样部56的第二次的采样结果的时点开始检测处理。异常检测部57判定上次的采样结果与本次的采样结果是否一致。在两采样结果不一致的情况下,异常检测部57判断为通信发生了异常,向处理部51通知检测到异常的内容。在两采样结果一致的情况下,异常检测部57将上次的采样结果废弃而存储本次的采样结果,并继续进行异常检测处理直至监视期间结束为止。

[0051] 在本实施方式中,需要采样部56的12次的采样结果全部一致,即,需要12次的采样结果全部为显性(0)或者全部为隐性(1)。在12次的采样结果中哪怕包含一次不同的值的情况下,监视装置5就判断为通信发生了异常。

[0052] 从CAN通信部53的异常检测部57被通知了检测出异常的处理部51进行异常通知处理部61对于通信系统中的全部的ECU3通知异常发生的处理。在本实施方式中,异常通知处理部61使CAN通信部53发送CAN协议中的错误帧,由此对于全部的ECU3通知异常发生。即使在基于ECU3的消息(数据帧)的发送中,也将其重写的形态进行错误帧的发送。监视装置5发送的错误帧被经由CAN总线连接的全部的ECU3接收。由此,能够阻碍检测到异常的消息被ECU3接收的情况。

[0053] <状态转换及流程图>

[0054] 图5是用于说明基于监视装置5的监视处理的状态转换图。本实施方式的监视装置5的CAN通信部53一边对同步状态St0、第一监视状态St1及第二监视状态St2这3个状态进行转换,一边进行监视处理。需要说明的是,同步状态St0相当于消息的SS及PTS的期间,第一监视状态St1相当于PBS1的期间,第二监视状态St2相当于PBS2的期间。CAN通信部53在监视处理中使用用于对T<sub>q</sub>数进行计数的计数器,但是这可以利用设置在CAN通信部53内的寄存器等的存储区域来实现。而且,CAN通信部53与周期T<sub>q</sub>的采样时钟同步地进行监视处理,对于每个1T<sub>q</sub>进行条件判定及状态转换等。

[0055] 在开始了对于CAN总线的消息发送的情况下,CAN通信部53将计数器的值初始化为0,开始同步状态St0下的处理。需要说明的是,在使基于CAN通信部53的监视处理开始的消息发送中,除了搭载于车辆1的正规的ECU3的消息发送之外,还能够包括例如对于CAN总线以不正当的方法连接的不正当的装置的消息发送等。

[0056] 在同步状态St0下,CAN通信部53判定转换条件1是否成立。转换条件1是向第一监视状态St1进行状态转换的条件,在本例中,以计数器的值达到SS的T<sub>q</sub>数及PTS的T<sub>q</sub>数的总计值的情况为条件。在转换条件1不成立的情况下,CAN通信部53使计数器的值增加(向计数器的值加1),并维持同步状态St0。在转换条件1成立的情况下,CAN通信部53将计数器的值初始化为0,将状态向第一监视状态St1转换。

[0057] 在第一监视状态St1下,CAN通信部53判定转换条件2是否成立。转换条件2是向第二监视状态St2进行状态转换的条件,在本例中,以计数器的值达到PBS1的T<sub>q</sub>数的情况为条件。需要说明的是,在本实施方式中,监视装置5的各段的长度采用与在通信系统中以最早的定时进行采样的ECU3a相同的值。即,根据图4,监视装置5的SS为1T<sub>q</sub>,PTS为3T<sub>q</sub>,PBS1为4T<sub>q</sub>,PBS2为8T<sub>q</sub>。由此,转换条件2是计数器的值达到4。但是,该段长度是一例,也可以采用



其他的值。

[0058] 在转换条件2不成立的情况下,CAN通信部53判定是否为第一监视状态St1下的第一次的处理。CAN通信部53根据计数器的值是否为0,能够判定是否为第一次的处理。在为第一次的处理的情况下,CAN通信部53进行采样部56对CAN总线的信号的采样,取得采样结果并存储于内部的寄存器等,并使计数器增加,维持第一监视状态St1。

[0059] 在为第二次以后的处理的情况下,CAN通信部53取得采样部56的采样结果,并判定上次的采样结果与本次的采样结果是否一致。在两采样结果一致的情况下,CAN通信部53将上次的采样结果废弃而存储本次的采样结果,并使计数器增加,维持第一监视状态St1。在两采样结果不一致的情况下,CAN通信部53向处理部51进行检测到异常的内容的通知,结束监视处理。需要说明的是,CAN通信部53在结束监视处理的情况下,可以从图5所示的状态转换脱离,也可以维持第一监视状态St1。

[0060] 在转换条件2成立的情况下,CAN通信部53将计数器的值初始化为0,将状态向第二监视状态St2转换。在第二监视状态St2下,CAN通信部53判定转换条件3是否成立。转换条件3是向同步状态St0进行状态转换的条件,在本例中,以计数器的值达到PBS2的T<sub>q</sub>数的情况为条件。需要说明的是,在本实施方式中,转换条件2是计数器值达到8。

[0061] 在转换条件3不成立的情况下,CAN通信部53取得采样部56的采样结果,并判定上次的采样结果与本次的采样结果是否一致。在两采样结果一致的情况下,CAN通信部53将上次的采样结果废弃而存储本次的采样结果,并使计数器增加,维持第二监视状态St2。在两采样结果不一致的情况下,CAN通信部53向处理部51进行检测到异常的内容的通知,结束监视处理。需要说明的是,CAN通信部53在结束监视处理的情况下,可以从图5所示的状态转换脱离,也可以维持第二监视状态St2。在转换条件3成立的情况下,CAN通信部53将计数器的值初始化为0,将状态向同步状态St0转换。

[0062] 这样CAN通信部53对3个状态进行转换而进行处理,由此能够将消息的一比特中的PBS1及PBS2作为监视期间来监视CAN总线上的信号的变化,能够检测与通信相关的异常。

[0063] 图6是表示监视装置5在同步状态St0下进行的处理的次序的流程图。需要说明的是,监视装置5的CAN通信部53例如与采样时钟等同步地,以1T<sub>q</sub>一次的频度执行本流程图所示的处理。在同步状态St0下,CAN通信部53判定转换条件1是否成立(步骤S1)。在转换条件1不成立的情况下(S1:否),CAN通信部53使计数器增加(步骤S2),并结束处理。在转换条件1成立的情况下(S1:是),CAN通信部53将计数器的值初始化为0(步骤S3),将状态向第一监视状态St1转换(步骤S4),结束处理。

[0064] 图7是表示监视装置5在第一监视状态St1中进行的处理的次序的流程图。在第一监视状态St1下,CAN通信部53首先进行采样部56对CAN总线的信号的采样,取得采样结果(步骤S11)。接下来,CAN通信部53判定转换条件2是否成立(步骤S12)。

[0065] 在转换条件2不成立的情况下(S12:否),CAN通信部53基于计数器的值,判定是否为第一监视状态St1下的第一次的处理(步骤S13)。在为第一次的处理的情况下(S13:是),CAN通信部53将由步骤S11取得的采样结果存储于内部的寄存器等(步骤S14),使计数器增加(步骤S15),并结束处理。

[0066] 在不是第一次的处理的情况下,即为第二次以后的处理的情况下(S13:否),CAN通信部53将上次的采样结果与本次的采样结果进行比较,判定两采样结果是否一致(步骤

S16)。在两采样结果一致的情况下(S16:是),CAN通信部53将由步骤S11取得的采样结果存储于内部的寄存器等(步骤S14),使计数器增加(步骤S15),并结束处理。

[0067] 在两采样结果不一致的情况下(S16:否),CAN通信部53向处理部51通知检测到异常的内容(步骤S17)。CAN通信部53结束监视处理(步骤S18),并结束第一监视状态St1中的处理。

[0068] 在转换条件2成立的情况下(S12:是),CAN通信部53将由步骤S11取得的采样结果存储于内部的寄存器等(步骤S19),将计数器的值初始化为0(步骤S20)。CAN通信部53将状态向第二监视状态St2转换(步骤S21),结束处理。

[0069] 图8是表示监视装置5在第二监视状态St2下进行的处理的次序的流程图。在第二监视状态St2下,CAN通信部53首先进行采样部56对CAN总线的信号的采样,取得采样结果(步骤S31)。接下来,CAN通信部53判定转换条件3是否成立(步骤S32)。

[0070] 在转换条件3不成立的情况下(S32:否),将上次的采样结果与本次的采样结果进行比较,并判定两采样结果是否一致(步骤S33)。在两采样结果一致的情况下(S33:是),CAN通信部53将由步骤S31取得的采样结果存储于内部的寄存器等(步骤S34),使计数器增加(步骤S35),结束处理。

[0071] 在两采样结果不一致的情况下(S33:否),CAN通信部53向处理部51通知检测到异常的内容(步骤S36)。CAN通信部53结束监视处理(步骤S37),结束第二监视状态St2下的处理。

[0072] 在转换条件3成立的情况下(S32:是),CAN通信部53将计数器的值初始化为0(步骤S38),将状态向同步状态St0转换(步骤S39),结束处理。

[0073] <总结>

[0074] 本实施方式的通信系统对于多个ECU3经由共用的通信线而进行信息的发送接收的系统结构,利用与该通信线连接的监视装置5进行与通信相关的异常检测。各ECU3在一比特的信息的发送期间中,以规定的定时进行一次采样,由此来接收信息。但是,容许多个ECU3以不同的定时进行采样的情况。监视装置5在一比特的信息的发送期间,在包含基于ECU3的最早的采样的定时和最晚的采样的定时的规定的监视期间,对通信线的电压进行多次采样。监视装置5能够在通信系统所包含的多个ECU3可进行采样的期间监视共用的通信线的电压的变化等,能够基于多次的采样的结果进行异常检测。

[0075] 监视装置5在规定的监视期间,周期性地多次采样,在上次的采样结果与本次的采样结果不同的情况下,即在规定的期间中通信线的信号变化的情况下,判断为通信发生了异常。由此,能够检测对应于特定的ECU3的采样定时而使信号变化所引起的信息篡改。

[0076] 另外,监视装置5在检测到与通信相关的异常的情况下,向多个ECU3进行通知。监视装置5例如对于通信线输出CAN协议的错误帧等,通过进行规定的信息发送而能够通知异常的发生。而且,在本通信系统中,通过基于监视装置5的异常通知用的信息发送,在通信系统中的各ECU3中能阻碍信息的接收。由此,能够防止篡改后的信息被ECU3接收的情况。

[0077] 需要说明的是,在本实施方式中,设为监视装置5将各ECU3的段的长度及采样定时等的信息作为定时信息52a而预先存储于存储部52的结构,但是并不局限于此。例如监视装置5也可以是不存储每个ECU3的定时等的信息而仅是存储监视期间的设定的结构。而且,在本实施方式中,将监视期间设为使PBS1及PBS2相加而得到的期间,但是并不局限于此。监视

期间例如在图4中可以将最早的采样定时设定作为开始时点并将最晚的采样定时设定作为结束时点,也可以是除此以外的期间。而且,监视装置5设为在监视期间中进行Tq单位下的采样(即,以1Tq一次的频度的采样)的结构,但是并不局限于此。监视装置5例如也可以设为以处理部31或CPU等生成的时钟单位进行采样的结构,还可以设为以其他的周期进行采样的结构。

[0078] 另外,监视装置5设为在监视期间中将上次的采样结果与本次的采样结果进行比较来进行异常检测的结构,但是并不局限于此。监视装置5例如也可以在一监视期间中预先保持初次的采样结果,将初次的采样结果与本次的采样结果进行比较,在本次的采样结果与初次的采样结果不同的情况下判断为发生了异常。监视装置5可以将本次的采样结果与以前的采样结果进行比较,在本次的采样结果与以前的采样结果不同的情况下,判断为发生了异常。

[0079] 另外,本实施方式的通信系统设为与ECU3不同的监视装置5进行异常检测的结构,但是并不局限于此。也可以具备对于通信系统所包含的多个ECU3中的任一个或多个ECU3进行异常检测的功能。而且,监视装置5设为在检测到与通信相关的异常的情况下发送错误帧而向ECU3通知异常的结构,但是并不局限于此,也可以设为通过错误帧的发送以外的方法进行异常通知的结构。而且,在本实施方式中,以搭载于车辆1的通信系统为例进行了说明,但是通信系统并不局限于向车辆1搭载的结构,例如也可以是搭载于飞机或船舶等移动体的结构,而且,例如还可以不是移动体而是设置于工厂、办公室或学校等的结构。

[0080] 标号说明

[0081] 1 车辆

[0082] 3 ECU(通信装置)

[0083] 5 监视装置(异常检测装置)

[0084] 31 处理部

[0085] 32 ROM

[0086] 33 RAM

[0087] 34 CAN通信部

[0088] 35 发送部

[0089] 36 接收部

[0090] 51 处理部

[0091] 52 存储部

[0092] 52a 定时信息

[0093] 53 CAN通信部

[0094] 54 发送部

[0095] 55 接收部

[0096] 56 采样部

[0097] 57 异常检测部(检测部)

[0098] 61 异常通知处理部(通知部)

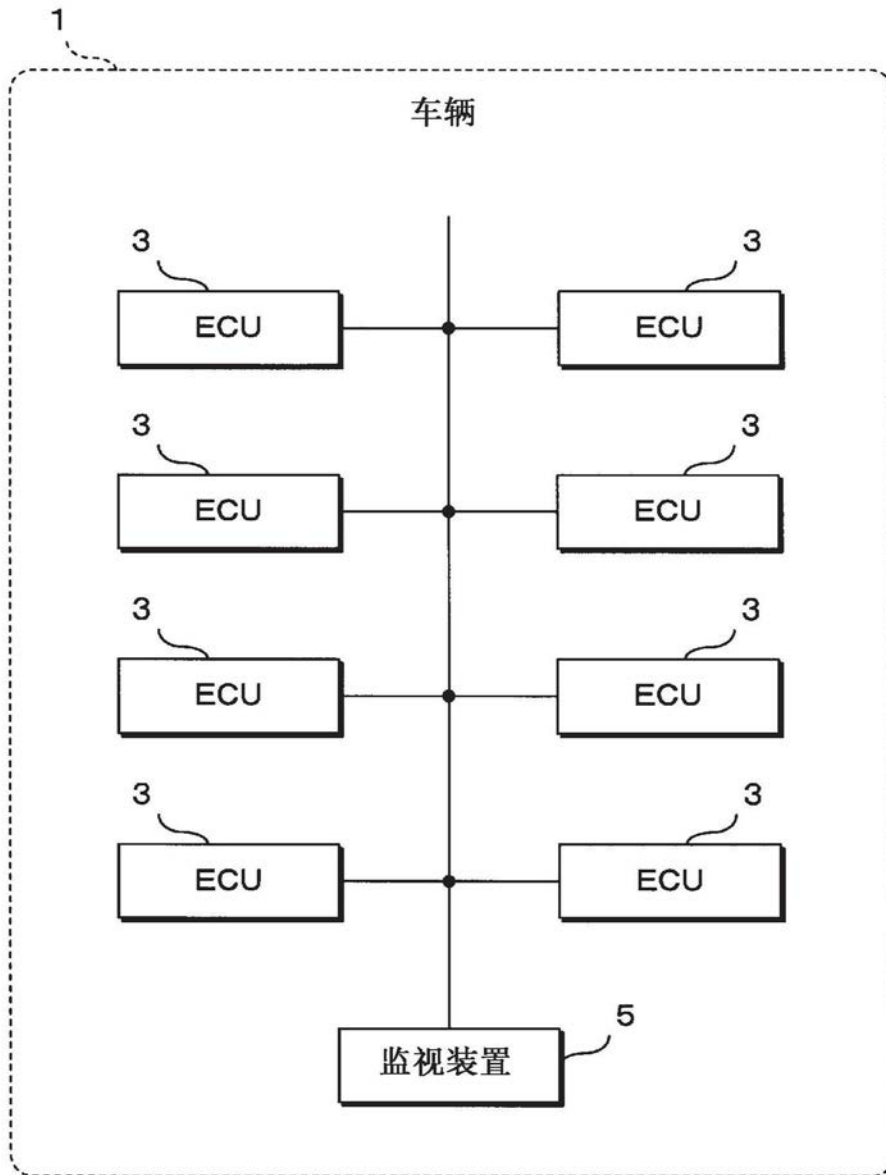


图1

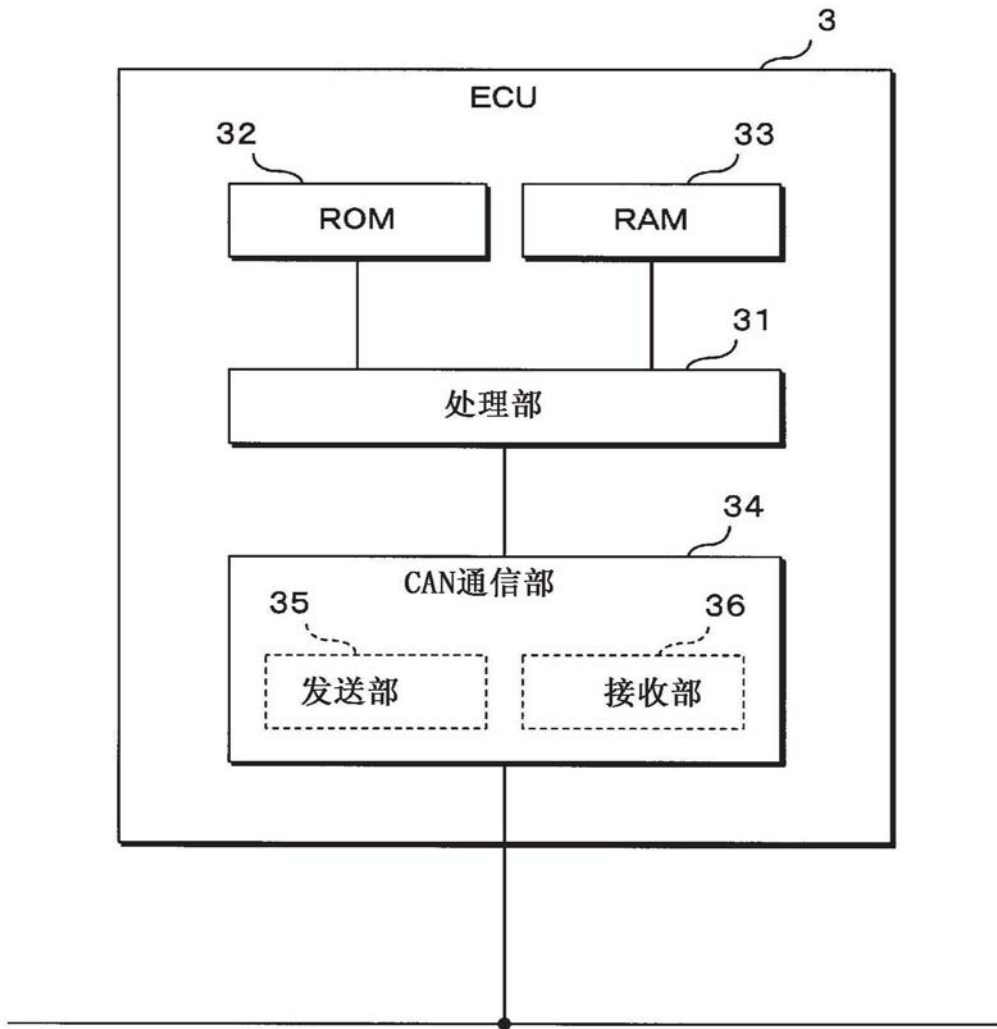


图2

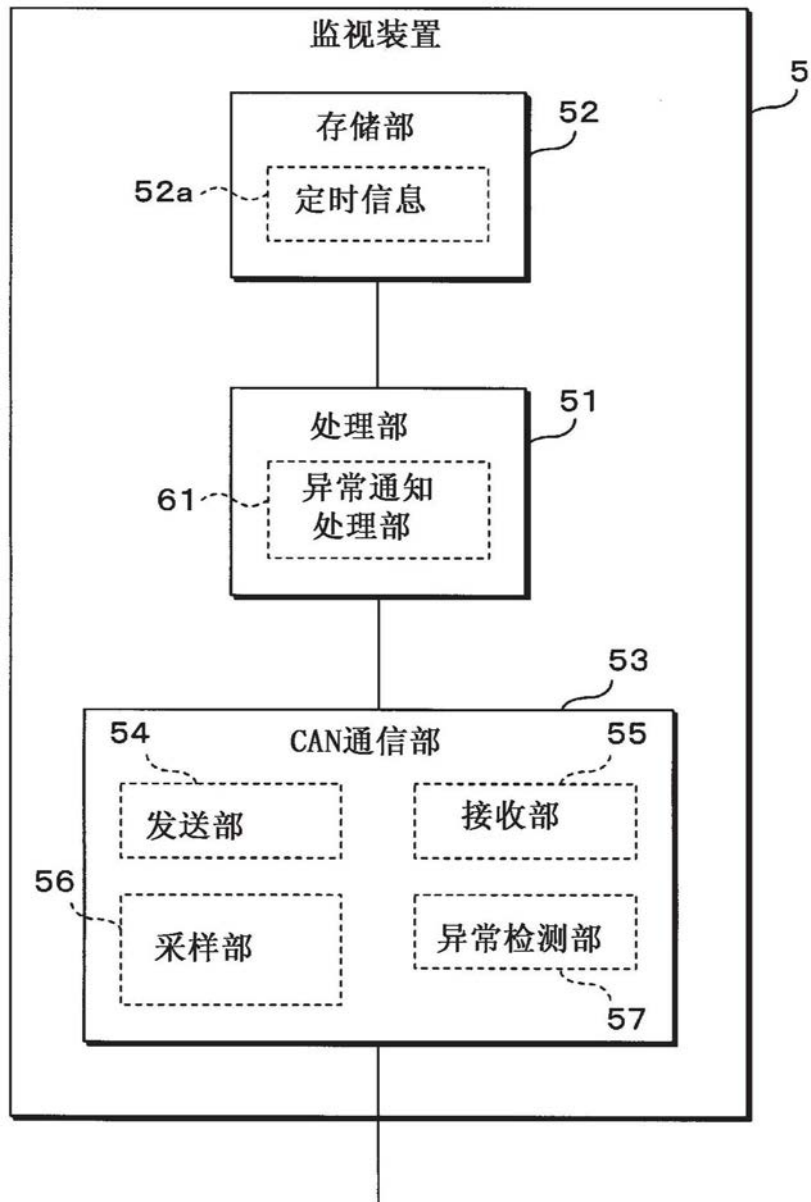


图3

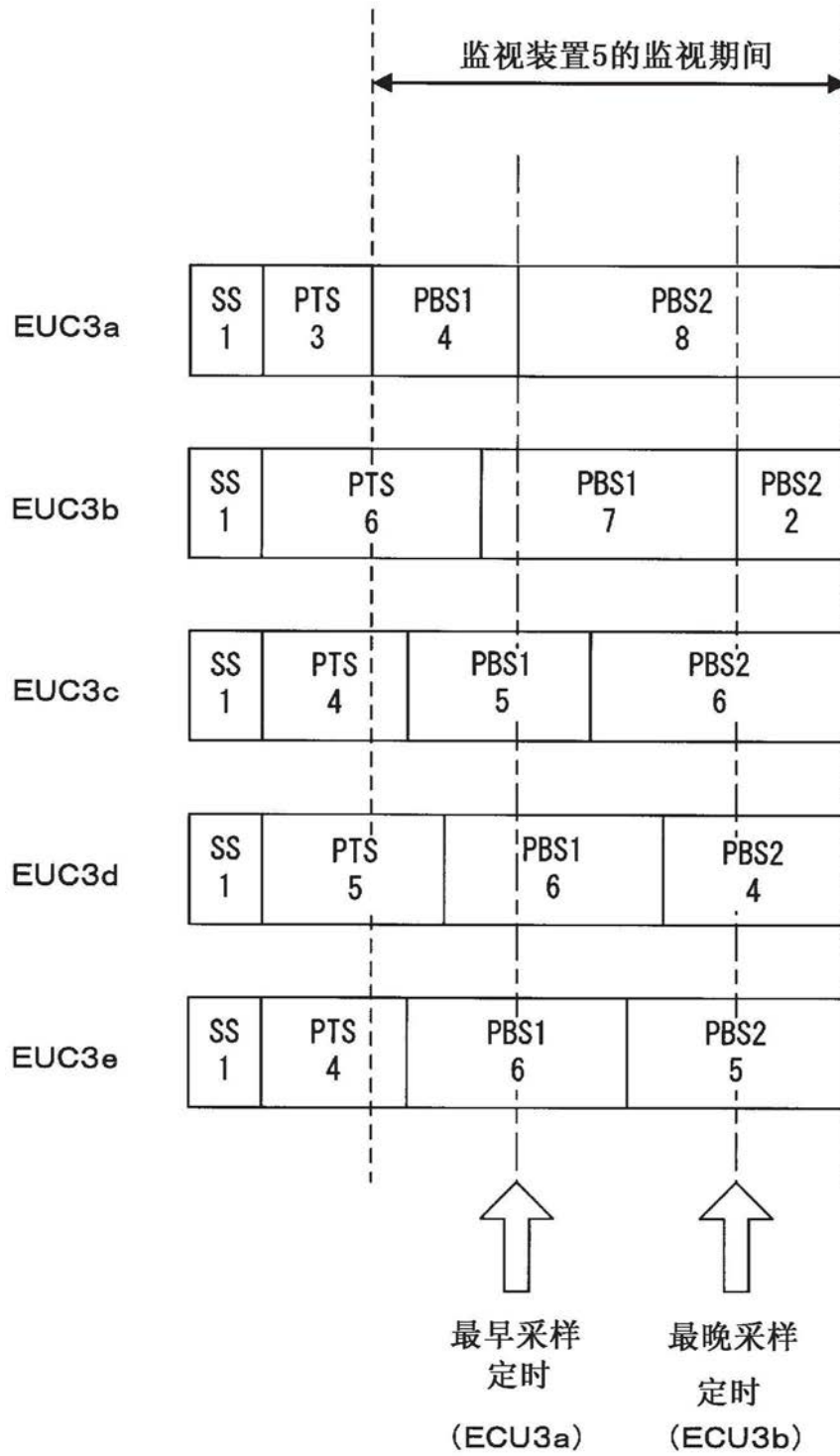


图4

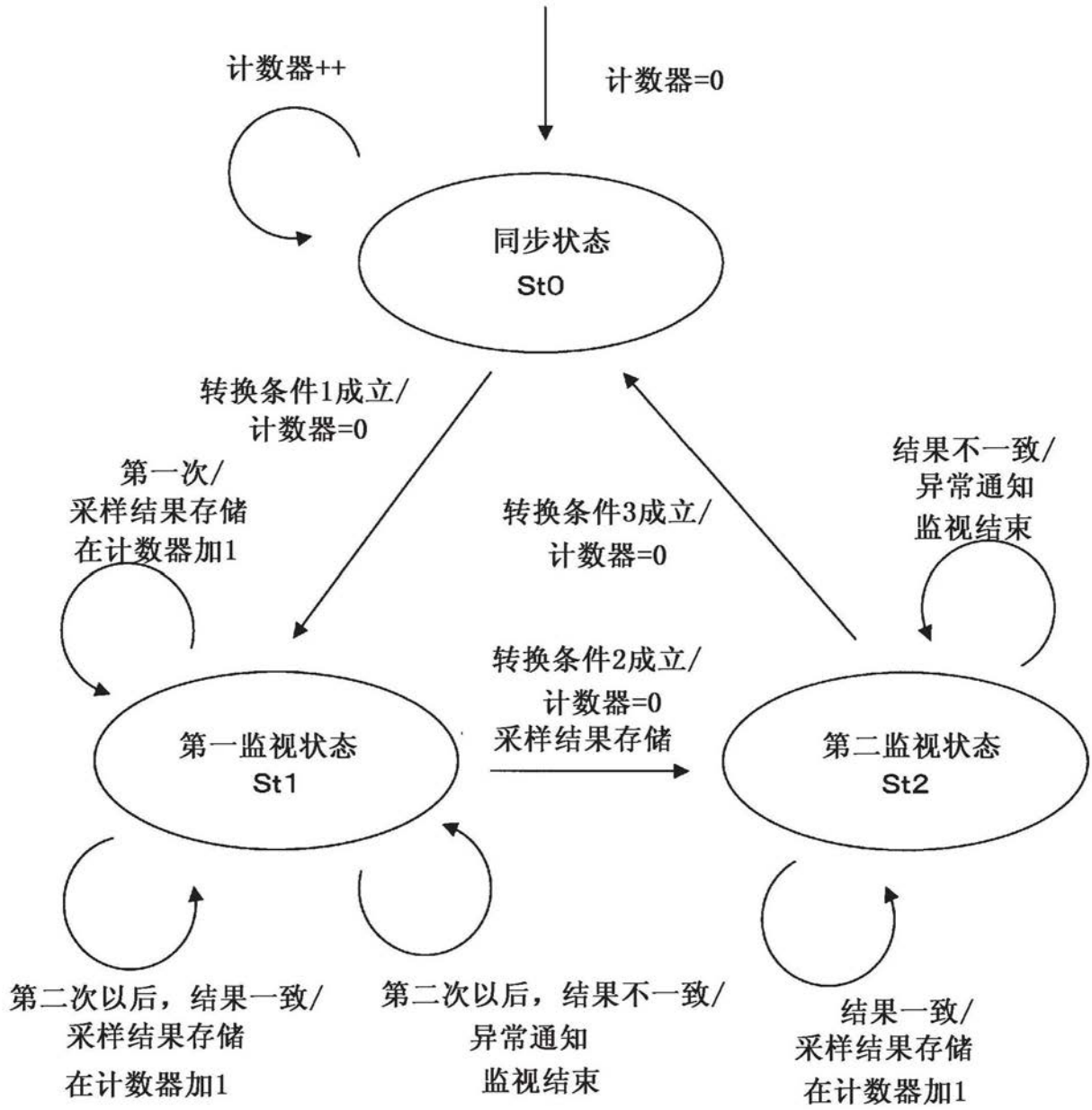


图5



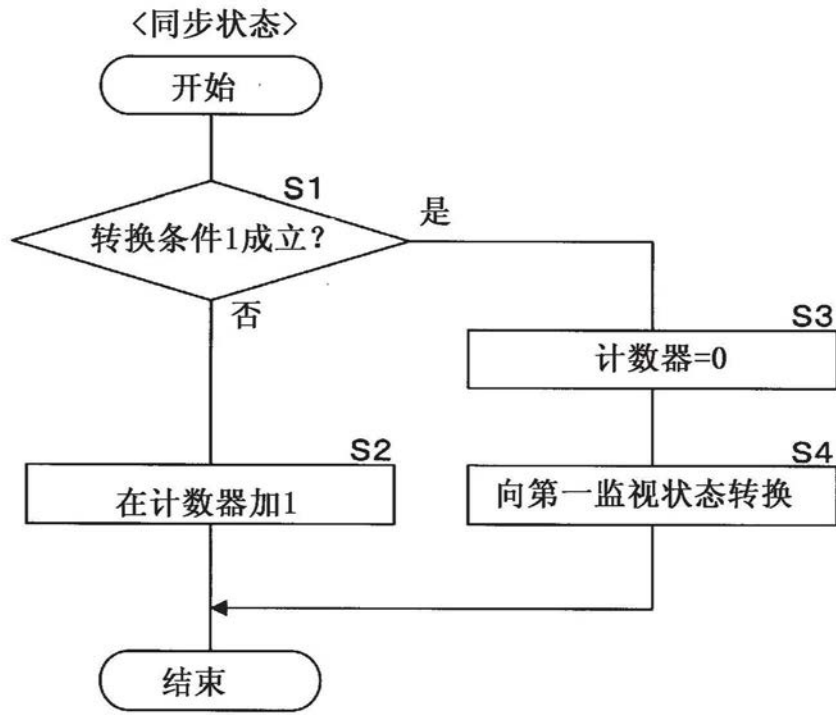


图6

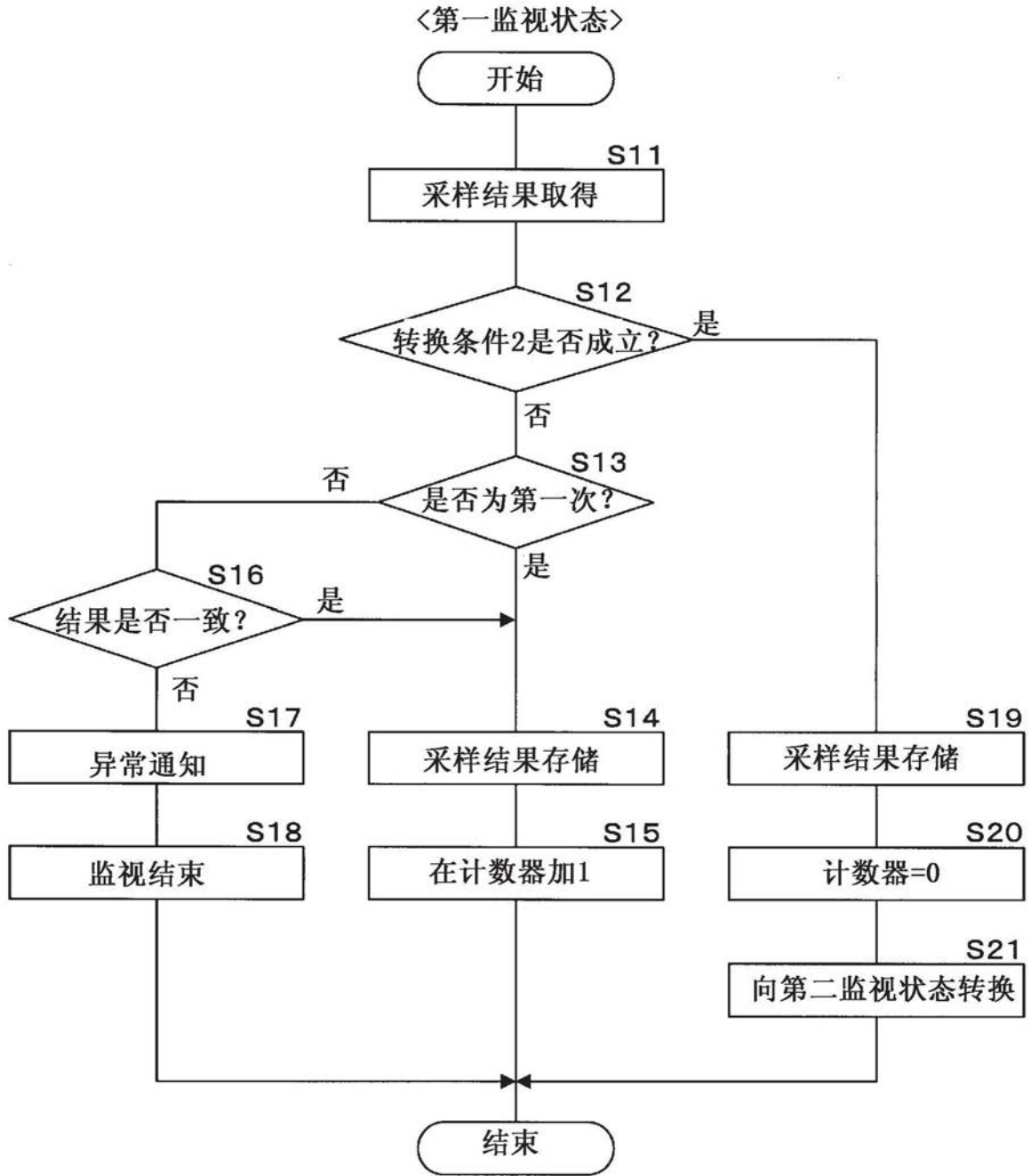


图7

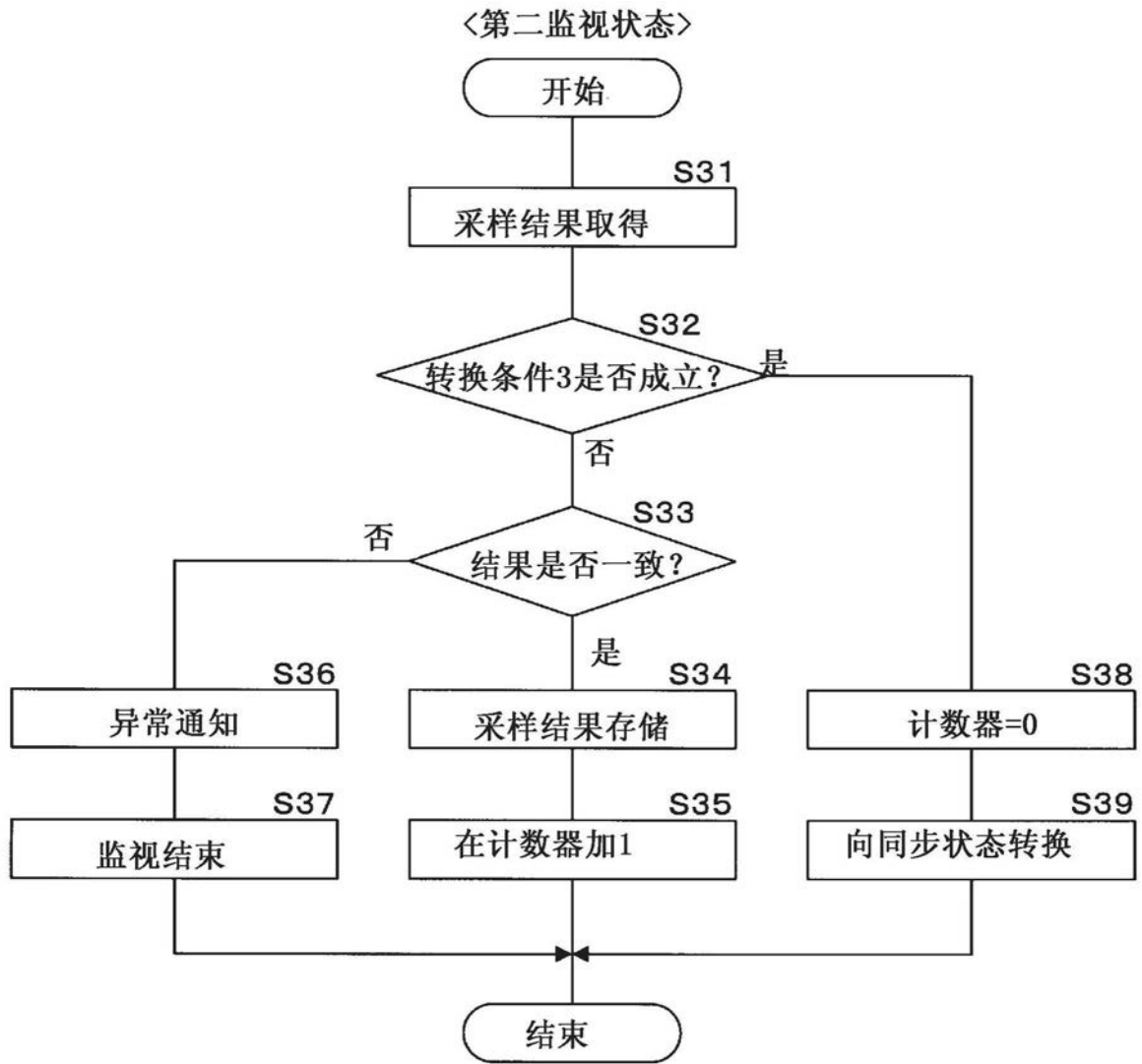


图8