



(21) 申请号 201910838205.X

(22) 申请日 2019.09.05

(65) 同一申请的已公布的文献号

申请公布号 CN 112447033 A

(43) 申请公布日 2021.03.05

(73) 专利权人 比亚迪股份有限公司

地址 518118 广东省深圳市坪山新区比亚迪路3009号

(72) 发明人 邓喜年 杨耕田

(74) 专利代理机构 深圳众鼎专利商标代理事务所(普通合伙) 44325

专利代理师 黄章辉

(51) Int.Cl.

G08B 25/14 (2006.01)

G08B 13/196 (2006.01)

H04L 12/46 (2006.01)

H04L 9/40 (2022.01)

H04L 67/12 (2022.01)

H04L 67/025 (2022.01)

H04N 7/18 (2006.01)

(56) 对比文件

CN 104125095 A, 2014.10.29

CN 105204471 A, 2015.12.30

CN 109255937 A, 2019.01.22

JP 2010134724 A, 2010.06.17

KR 20190057818 A, 2019.05.29

CN 108572606 A, 2018.09.25

CN 107481472 A, 2017.12.15

CN 107864174 A, 2018.03.30

CN 106656632 A, 2017.05.10

CN 109544879 A, 2019.03.29

CN 109215264 A, 2019.01.15

CN 1412686 A, 2003.04.23

CN 107632285 A, 2018.01.26

CN 105491066 A, 2016.04.13

CN 110191478 A, 2019.08.30

肖立中; 刘云翔; 戴蒙. 入侵检测系统中分层报警处理模型的研究. 计算机应用研究. 2009, (第08期), 2995-2999.

审查员 李钢

权利要求书3页 说明书15页 附图12页

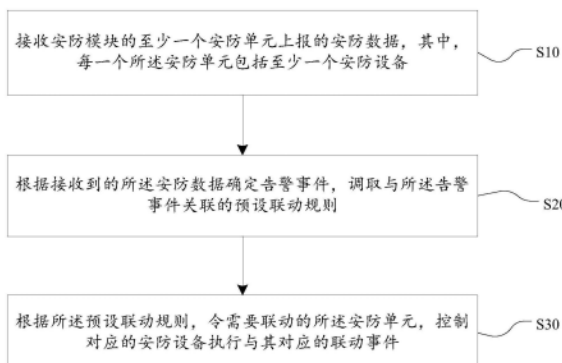
(54) 发明名称

安防数据处理方法、系统、计算机设备及存储介质

(57) 摘要

本发明公开了一种安防数据处理方法、系统、计算机设备及存储介质。所述方法包括:接收安防模块的至少一个安防单元上报的安防数据,其中,每一个所述安防单元包括至少一个安防设备;根据接收到的所述安防数据确定告警事件,调取与所述告警事件关联的预设联动规则;根据所述预设联动规则,令需要联动的所述安防单元,控制对应的安防设备执行与其对应的联动事件。本发明通过对不同用途的安防单元的安防数据进行统一处理,调动整个车站的各安防单元的安防设备针对告警事件执行与联动事件,提升了车站对于告警事件的处理效率,使告警事件可以

得到及时控制和稳妥处理,保证了车站的安全高效运行。



1. 一种安防数据处理方法,其特征在于,包括:

接收安防模块的至少一个安防单元上报的安防数据,其中,每一个所述安防单元包括至少一个安防设备;

所述接收安防模块的至少一个安防单元上报的安防数据,包括:

接收安防模块的至少一个安防单元通过MQTT中间件上报的安防数据,并将上报的所述安防数据经过封装处理之后,按照预设的插入规则插入待处理消息队列中;所述预设的插入规则为按照处理完成的时间点的时间顺序或按照数据类型排序;

根据接收到的所述安防数据确定告警事件,调取与所述告警事件关联的预设联动规则;其中,所述预设联动规则中包括所有需要联动的所述安防单元的属性以及需要联动的所述安防单元中的所有需要联动的所述安防设备的待执行的联动事件;

根据所述预设联动规则,令需要联动的所述安防单元,控制对应的安防设备执行与其对应的联动事件;

所述根据接收到的所述安防数据确定告警事件之后,还包括:

将与所述安防数据进行再次封装处理之后对应的告警事件插入告警队列中,记录与所述告警事件对应的所述安防设备的当前运行状态,并将所述当前运行状态通过WebSocket发送到决策模块进行实时显示,同时在所述决策模块中对与所述安防数据对应的所述告警事件进行警示。

2. 如权利要求1所述的安防数据处理方法,其特征在于,所述安防单元包括视频监控单元、入侵监控单元、出入口监控单元、安检单元和电子巡检单元中的至少一种;

所述安防数据包括以下数据中的至少一种:

所述视频监控单元根据预设的布防信息,对摄像设备拍摄的视频信息进行分析之后获取的视频监控数据;

所述入侵监控单元的入侵监控设备,对车站的预设禁止区域的入侵监控数据;

所述出入口监控单元的出入口监控设备,对车站出入口进行监控的通行数据;

所述安检单元的安检设备,对车站进行安检的安检数据,所述安检数据包括安检图像或/和危险品检测信息;

所述电子巡检单元的巡检设备,根据巡检计划中的各巡检点的巡检路线,进行巡检之后的巡检数据。

3. 如权利要求1所述的安防数据处理方法,其特征在于,所述根据接收到的所述安防数据确定告警事件,包括:

自所述待处理消息队列中按照预设的解析顺序调取所述安防数据;

解析所述安防数据的类型和数据值,并获取与所述安防数据的类型关联的告警阈值;

在所述安防数据的数据值超过所述告警阈值时,根据所述安防数据的数据值确认与所述安防数据对应的告警事件。

4. 如权利要求1所述的安防数据处理方法,其特征在于,所述根据所述预设联动规则,令需要联动的所述安防单元,控制对应的安防设备执行与其对应的联动事件之后,包括:

获取各所述安防设备执行所述联动事件之后的执行结果,通过WebSocket将所述执行结果发送到决策模块进行实时显示,并根据所述执行结果调整与所述告警事件关联的所述预设联动规则。

5. 如权利要求3所述的安防数据处理方法,其特征在于,所述解析所述安防数据的类型和数据值之后,还包括:

获取与所述安防数据的类型关联的存储区域,将所述安防数据存储至与其关联的存储区域,并在存储完成之后接收反馈的处理完毕回执。

6. 如权利要求1所述的安防数据处理方法,其特征在于,所述调取与所述告警事件关联的预设联动规则之前,还包括:

为所述预设联动规则分配对应的所述安防单元,并将所述安防单元与所述预设联动规则关联;

根据所述预设联动规则,为所述安防单元中对应的所述安防设备配置联动事件;

将每一项所述预设联动规则与至少一项告警事件关联。

7. 如权利要求1所述的安防数据处理方法,其特征在于,还包括:

接收登录用户发送的登录请求,自数据库中调取登录权限信息;所述登录权限信息中包括允许登录用户信息以及与每一项所述允许登录用户信息关联的允许登录区域;

若所述登录请求中包括的登录用户信息与所述允许登录用户信息匹配,根据所述允许登录用户信息关联的所述允许登录区域,对所述登录用户开放所述允许登录区域的访问权限。

8. 如权利要求1所述的安防数据处理方法,其特征在于,还包括:

接收车站展示指令,将车站的构造图以及所述车站中的所有车站安防设备,以二维、三维形式中的至少一种展示在当前显示界面。

9. 如权利要求1所述的安防数据处理方法,其特征在于,还包括:

接收包括安防设备的设备参数的设备配置指令,根据所述设备参数将所述安防设备配置至所述安防模块下的所述安防单元。

10. 一种安防数据处理系统,其特征在于,包括安防模块和与所述安防模块通信连接的物联网控制模块,所述安防模块包括至少一个安防单元,每一个所述安防单元包括至少一个安防设备;

所述物联网控制模块包括:

接收单元,用于接收安防模块的至少一个安防单元上报的安防数据,其中,每一个所述安防单元包括至少一个安防设备;

所述接收单元,还包括:接收安防模块的至少一个安防单元通过MQTT中间件上报的安防数据,并将上报的所述安防数据经过封装处理之后,按照预设的插入规则插入待处理消息队列中;所述预设的插入规则为按照处理完成的时间点的时间顺序或按照数据类型排序;

调取单元,用于根据接收到的所述安防数据确定告警事件,调取与所述告警事件关联的预设联动规则;其中,所述预设联动规则中包括所有需要联动的所述安防单元的属性以及需要联动的所述安防单元中的所有需要联动的所述安防设备的待执行的联动事件;

执行单元,用于根据所述预设联动规则,令需要联动的所述安防单元,控制对应的安防设备执行与其对应的联动事件;

所述调取单元,还包括:

将与所述安防数据进行再次封装处理之后对应的告警事件插入告警队列中,记录与所

述告警事件对应的所述安防设备的当前运行状态,并将所述当前运行状态通过WebSocket发送到决策模块进行实时显示,同时在所述决策模块中对与所述安防数据对应的所述告警事件进行警示。

11.一种计算机可读存储介质,所述计算机可读存储介质存储有计算机可读指令,其特征在于,所述计算机可读指令被处理器执行时实现如权利要求1至9任一项所述安防数据处理方法。

## 安防数据处理方法、系统、计算机设备及存储介质

### 技术领域

[0001] 本发明涉及安防数据处理领域,具体涉及一种安防数据处理方法、系统、计算机设备及存储介质。

### 背景技术

[0002] 随着科学技术的发展,现代城市轨道交通发展迅速,而安防系统作为现代城市轨道交通中车站必不可少的一部分,可以为运营和管理人员提供并记录车站的各种安防信息,以对车站的运行进行安全管理,辅助维护车站安全。在现有技术中,车站中的安防系统主要是依赖视频监控系统、出入口控制系统等,由于,不同系统各自独立运行,各系统之间的数据无法同时被查看,也无法综合评估车站的安防运行状态,因此,各系统仅会根据本系统的运行数据针对系统内紧急事件的告警的制定不同应对措施,如此,由于无法综合各系统的数据对于紧急事件的告警进行综合处理,可能会导致各系统对于紧急事件的告警的最终应对措施的不全面稳妥,进而导致安防系统的紧急事件无法得到及时的控制和解决。

### 发明内容

[0003] 本发明实施例提供一种安防数据处理方法、系统、计算机设备及存储介质,可以对不同用途的安防单元发送的安防数据进行统一处理,并通过综合处理安防数据确定告警事件之后,按照预设联动规则对该告警事件进行处理;使得整个车站的安防运行状态更为清晰,告警事件亦可以得到及时控制和稳妥处理,提升了告警事件处理效率,保证了车站的安全高效运行。

[0004] 一种安防数据处理方法,包括:

[0005] 接收安防模块的至少一个安防单元上报的安防数据,其中,每一个所述安防单元包括至少一个安防设备;

[0006] 根据接收到的所述安防数据确定告警事件,调取与所述告警事件关联的预设联动规则;

[0007] 根据所述预设联动规则,令需要联动的所述安防单元,控制对应的安防设备执行与其对应的联动事件。

[0008] 一种安防数据处理系统,包括安防模块和与所述安防模块通信连接的物联网控制模块,所述安防模块包括至少一个安防单元,每一个所述安防单元包括至少一个安防设备;

[0009] 所述物联网控制模块包括:

[0010] 接收单元,用于接收安防模块的至少一个安防单元上报的安防数据,其中,每一个所述安防单元包括至少一个安防设备;

[0011] 调取单元,用于根据接收到的所述安防数据确定告警事件,调取与所述告警事件关联的预设联动规则;

[0012] 执行单元,用于根据所述预设联动规则,令需要联动的所述安防单元,控制对应的安防设备执行与其对应的联动事件。

[0013] 一种计算机可读存储介质,所述计算机可读存储介质存储有计算机可读指令,所述计算机可读指令被处理器执行时实现上述安防数据处理方法。

[0014] 本发明提供的安防数据处理方法、系统、计算机设备及存储介质,本发明的安防数据处理系统中包括通信连接的安防模块和物联网控制模块,且不同用途的安防单元均集成在安防模块中,如此,可以在物联网控制模块中对不同用途的安防单元的安防数据进行统一处理,并通过综合处理安防数据确定告警事件并按照预设联动规则对该告警事件进行处理;如此,一方面,对不同用途的安防单元的安防数据进行统一处理,使得整个车站的安防运行状态更为清晰,可以令车站运营人员更清楚地了解整个车站的安防运行状态,进而可以对各种告警及紧急事件及时进行分析评估处理,这对整个车站的安防工作有很大的帮助和提升;另一方面,通过综合处理安防数据确定告警事件并按照预设联动规则对该告警事件进行处理,可以调动整个车站的各安防单元的安防设备联动执行与其对应的所述联动事件,大大提升了车站对于告警事件的处理效率,使告警事件可以得到及时控制和稳妥处理,保证了车站的安全高效运行。

## 附图说明

[0015] 为了更清楚地说明本发明实施例的技术方案,下面将对本发明实施例的描述中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本发明的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图获得其他的附图。

[0016] 图1是本发明一实施例中安防数据处理方法的流程图;

[0017] 图2是本发明一实施例中安防数据处理系统的原理框图;

[0018] 图3是本发明一实施例中安防数据处理系统的安防模块的原理框图;

[0019] 图4是本发明另一实施例中安防数据处理系统的原理框图;

[0020] 图5是本发明一实施例中安防数据处理系统的调取单元的原理框图;

[0021] 图6是本发明又一实施例中安防数据处理系统的原理框图;

[0022] 图7是本发明再一实施例中安防数据处理系统的原理框图;

[0023] 图8是本发明另一实施例中安防数据处理系统的调取单元的原理框图;

[0024] 图9是本发明一实施例中安防数据处理系统的物联网控制模块的原理框图;

[0025] 图10是本发明另一实施例中安防数据处理系统的物联网控制模块的原理框图;

[0026] 图11是本发明又一实施例中安防数据处理系统的物联网控制模块的原理框图;

[0027] 图12是本发明一实施例中安防数据处理系统的架构原理框图;

[0028] 图13是本发明另一实施例中安防数据处理系统的架构原理框图;

[0029] 图14是本发明另一实施例中安防数据处理系统中事件告警管理模块的原理框图;

[0030] 图15是本发明一实施例中计算机设备的示意图。

## 具体实施方式

[0031] 下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例是本发明一部分实施例,而不是全部的实施例。基于本发明中的实施例,本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施

例,都属于本发明保护的范围。

[0032] 如图1所示,本发明提供一种安防数据处理方法,包括以下步骤S10-S30:

[0033] S10,接收安防模块的至少一个安防单元上报的安防数据,其中,每一个所述安防单元包括至少一个安防设备;可理解地,本发明上述安防数据处理方法应用于安防数据处理系统的物联网控制模块,且该物联网控制模块与所述安防模块通信连接。其中,安防模块中集成了至少一个安防单元,安防单元可以为视频监控单元、入侵监控单元、出入口监控单元、安检单元和电子巡检单元等的任意一个安防单元,而不局限于此,作为一个示例,安防模块中集成了多个安防单元,而由于安防模块中包括多个不同的安防单元,因此,安防模块中包括但不限于视频监控单元、入侵监控单元、出入口监控单元、安检单元和电子巡检单元中的至少两个安防单元。并且,每一个安防单元中都包括有安防单元可以直接进行控制的安防设备,安防设备包括但不限于以下设备:视频监控单元包括摄像设备,入侵监控单元包括入侵监控设备(比如可以检测是否有不允许通行的人员或物品入侵预设禁止区域的传感器等),出入口监控单元包括出入口监控设备(用于控制出入口的开关以及监测出入口的通行情况的设备),安检单元包括安检设备(用于获取和分析车站的安检图像或/和危险品检测信息等),电子巡检单元包括巡检设备(用于根据巡检计划中的各巡检点的巡检路线进行巡检),而不局限于此。

[0034] S20,根据接收到的所述安防数据确定告警事件,调取与所述告警事件关联的预设联动规则;其中,所述预设联动规则中包括所有需要联动的所述安防单元的属性以及需要联动的所述安防单元中的所有需要联动的所述安防设备的待执行的联动事件;也即,在接收到一个或者多个安防单元发送的安防数据之后,可以根据上述接收到的安防数据综合判定是否出现告警事件,若有出现告警事件,则首先确定该告警事件的属性(比如类型、名称、危险等级或紧要等级等属性),之后再从数据库(数据库中存储有安防数据处理系统中的需要保存的所有数据)中调取与告警事件的属性匹配的预设联动规则,并根据该预设联动规则确定需要联动的安防单元,以及各安防单元中的所有需要联动的所述安防设备及其待执行的联动事件,并进入步骤S30中。其中,联动事件是指一个安防设备在进行联动时需要执行的操作事件,比如,安防设备为出入口监控设备,所述联动事件可以是指所述出入口监控设备控制出入口的开关状态的切换。若数据库中没有与告警事件相关联的预设联动规则,可通过更新数据库,使数据库中具备与该告警事件对应的预设联动规则。

[0035] S30,根据所述预设联动规则,令需要联动的所述安防单元,控制对应的安防设备执行与其对应的联动事件。具体地,所述步骤S30中,可以根据所述预设联动规则,令需要联动的所述安防单元指示该安防单元中需要联动的各所述安防设备执行与其对应的所述联动事件。也即,在根据该预设联动规则确定需要联动的安防单元,以及各安防单元中的所有需要联动的所述安防设备及其待执行的联动事件之后,可以直接将各安防单元中的所有需要联动的所述安防设备及其待执行的联动事件分别发送给相应的安防单元,以供该安防单元根据接收到的信息指示各需要联动的所述安防设备执行各自的待执行的联动事件,如此,完成了通过综合分析安防数据对告警事件自动进行及时高效处理的过程,全程可以无需人工进行操作即可完成。

[0036] 本发明的不同用途的安防单元均集成在安防模块中,如此,本发明提供的安防数据处理方法可以对不同用途的安防单元的安防数据进行统一处理,并通过综合处理安防数

据确定告警事件并按照预设联动规则对该告警事件进行处理;如此,一方面,对不同用途的安防单元的安防数据进行统一处理,使得整个车站的安防运行状态更为清晰,可以令车站运营人员更清楚地了解整个车站的安防运行状态,进而可以对各种告警及紧急事件及时进行分析评估处理,这对整个车站的安防工作有很大的帮助和提升;另一方面,通过综合处理安防数据确定告警事件并按照预设联动规则对该告警事件进行处理,可以调动整个车站的各安防单元的安防设备联动执行与其对应的所述联动事件,大大提升了车站对于告警事件的处理效率,使告警事件可以得到及时控制和稳妥处理,保证了车站的安全高效运行。同时,通过对安防数据的有效管理,可以方便后续的系统维护与扩展。

[0037] 在一实施例中,所述安防单元包括视频监控单元、入侵监控单元、出入口监控单元、安检单元和电子巡检单元中的一种或多种;也即,一个所述安防单元可以为视频监控单元、入侵监控单元、出入口监控单元、安检单元和电子巡检单元中的任意一个,而安防模块中包括多个不同的安防单元,也即,安防模块中包括视频监控单元、入侵监控单元、出入口监控单元、安检单元和电子巡检单元中的任意多个安防单元,其中,多个为至少两个。

[0038] 作为优选,所述安防数据包括所述视频监控单元根据预设的布防信息,对摄像设备拍摄的视频信息进行分析之后获取的视频监控数据;此时,所述步骤S10中,所述接收安防模块的至少一个安防单元上报的安防数据,包括:

[0039] 接收所述视频监控单元发送的视频监控数据,所述视频监控数据是指视频监控单元根据预设的布防信息,对摄像设备拍摄的视频信息进行分析之后获取的分析数据(所述分析数据可以是指对视频信息中的图像进行人脸分析之后,确定当前视频中的预设区域内的人脸的数据,也即人员聚集情况,同时,该分析数据亦可以为对于视频信息中的物品的分析等);在本实施例中,可以通过视频监控单元的摄像设备拍摄视频信息,且该视频监控单元还可以进行视频预览,视频回放,云台控制及抓图等功能,还可以根据预先设置布防信息来对于摄像设备拍摄的视频信息进行智能分析,以在分析数据中表明人员聚集、物品遗留、徘徊侦测等事件的相关分析数据,以利于后续视频监控单元将该分析数据(也即视频监控数据)发送至物联网控制模块之后,可供物联网控制模块根据该分析数据确认其是否构成了告警事件,将上述获取分析数据的过程在该视频监控单元中进行(在另一实施例中,亦可以将该分析过程在物联网控制模块进行),是为了减小物联网控制模块(需要同时处理多种安防数据,数据处理量大)的负载,以提升其运行速率。进一步地,所述视频监控单元提供多种接口,比如,用于获取摄像设备拍摄的视频信息的视频信息接口,用于获取视频预览、视频回放、云台控制等控制信号(该控制信号可以由物联网控制模块发送至该控制接口,也可以根据用户对于视频监控单元的操作指令生成)的控制接口,对视频信息进行智能分析的配置布防接口等。

[0040] 进一步地,所述安防数据包括所述入侵监控单元的入侵监控设备,对车站的预设禁止区域的入侵监控数据;此时,所述步骤S10中,所述接收安防模块的至少一个安防单元上报的安防数据,包括:接收所述入侵监控单元发送的入侵监控数据,所述入侵监控数据是指所述入侵监控单元的入侵监控设备,对车站的预设禁止区域的监控数据;在本实施例中,可以通过入侵监控单元中的入侵监控设备获取根据检测布防计划对车站的边缘及黄线禁止区域等预设禁止区域进行监管的监控数据(也即入侵监控数据,所述监控数据可以是指指在预设禁止区域中是否存在不允许进入的人员或者物品、该预设禁止区域中存在的人员或

物品的数量等信息,上述入侵监控数据可以从被监控的该预设禁止区域的视频信息中分析得出,亦可以由该预设禁止区域的工作人员直接上报),以利于后续入侵监控单元将该监控数据发送至物联网控制模块之后,可供物联网控制模块根据该监控数据确认其是否构成了告警事件。进一步地,所述入侵监控单元中包括用于对预设禁止区域进行控制并获取入侵监控数据的管理接口,也包括可以将入侵监控单元中的入侵监控设备的告警事件上报至物联网控制模块的报警上报接口;也即,若根据入侵监控数据确认其是否为告警事件的过程,直接在入侵检测单元中进行,此时,在确认告警事件之后,也可直接通过该报警上报接口上报该告警事件,此时,可以将该告警事件视为上述上报的入侵监控数据的一部分。

[0041] 进一步地,所述安防数据包括所述出入口监控单元的出入口监控设备,对车站出入口进行监控的通行数据;此时,所述步骤S10中,所述接收安防模块的至少一个安防单元上报的安防数据,包括:接收所述出入口监控单元发送的通行数据,所述通行数据是指出入口监控单元的出入口监控设备,对车站的出入口的监控数据;在本实施例中,可以通过入口监控单元的出入口监控设备(控制出入口的开关以及监测出入口的通行情况的设备)获取对车站的出入口进行控制的监控数据(也即通行数据,上述通行数据可以是指出入口当前已通行人员的数量、正在出入口之前等待的通行人员数量、根据车站的车辆班次预估的将要通行的通行人员的数量等),以利于后续出入口监控单元将该通行数据发送至物联网控制模块之后,可供物联网控制模块根据该通行数据确认其是否构成了告警事件。可理解地,出入口的开关的控制指令可以由物联网控制模块直接发出,也即,物联网控制模块可以间接控制入口监控单元的出入口监控设备对车站出入口的开关状态。进一步地,所述入口监控单元提供有与所述物联网控制模块通信连接的指令控制接口,物联网控制模块下达的对于出入口的控制指令,可以通过该指令控制接口下发至入口监控单元,且入口监控单元根据物联网控制模块下达的对于出入口的控制指令控制出入口监控设备调整出入口的开关状态。

[0042] 进一步地,所述安防数据包括所述安检单元的安检设备,对车站进行安检的安检数据,所述安检数据包括安检图像或/和危险品检测信息;此时,所述步骤S10中,所述接收安防模块的至少一个安防单元上报的安防数据,包括:接收所述安检单元发送的安检数据,所述安检数据是指所述安检单元的安检设备,对车站的安检图像或/和危险品检测信息;在本实施例中,可以通过安检单元的安检设备获取和分析车站的安检图像或/和危险品检测信息(也即安检数据,所述安检数据包括当前检查的危险品的数量和种类、当前进行安检的人员或者物品的图像等),以利于后续安检单元将该安检数据发送至物联网控制模块之后,可供物联网控制模块根据该安检数据确认其是否构成了告警事件。也即,物联网控制模块可实时获取安检单元的安检设备获取的安检图像及其他信息,也可进行通过危险品检测信息实现对安检中的危险品管理。进一步地,所述安检单元提供可以获取实时安检图像或/和危险品检测信息的安检接口。

[0043] 进一步地,所述安防数据包括所述电子巡检单元的巡检设备,根据巡检计划中的各巡检点的巡检路线,进行巡检之后的巡检数据。此时,所述步骤S10中,所述接收安防模块的至少一个安防单元上报的安防数据,包括:接收所述电子巡检单元发送的巡检数据,所述巡检数据是指所述电子巡检单元的巡检设备,根据巡检计划中的各巡检点的巡检路线,进行巡检之后的巡检结果数据。在本实施例中,可以通过电子巡检单元的巡检设备获取根据

巡检计划中的各巡检点的巡检路线进行巡检之后的巡检结果数据(也即巡检数据,所述巡检数据是巡检人员根据巡检路线进行巡检时,确认该巡检路线上是否存在异常情况,若存在异常情况,需要附上该异常情况的具体信息,比如视频或者其他数据等),以利于后续电子巡检单元将该巡检数据发送至物联网控制模块之后,可供物联网控制模块根据该巡检数据确认其是否构成了告警事件。可理解地,电子巡检单元可以实现对、巡检点、巡检计划、巡检线路等的管理,也可以查看巡检结果以及巡检报告,并将其发送至物联网控制模块实时查看和分析。进一步地,电子巡检单元提供获取巡查线路,巡查计划及巡查结果等信息的巡检接口。

[0044] 进一步的,上述安防模块的安防单元中的各接口(比如视频信息接口、控制接口、配置布防接口、管理接口、报警上报接口、指令控制接口、安检接口、巡检接口等)优选为API接口(Application Programming Interface,应用程序编程接口)。应用程序API是一些预先定义的函数,可以提供应用程序给开发人员基于某软件或硬件得以访问一组例程的能力,而又无需访问源码,或理解内部工作机制的细节。

[0045] 由以上可知,各安防单元均可以各自获取该安防单元内的安防设备的安防数据,并将该安防数据上报给物联网控制模块,物联网控制模块可以根据上述接收到的所有的安防数据进行综合分析,多重确认当前的安防数据是否对应于告警事件的发生,并对告警事件等不同状况进行预防和及时应对;同时,还可以通过对告警事件相关数据进行进一步评估,为整个车站的更好运营决策提供帮助。

[0046] 在一实施例中,所述步骤S10中,所述接收安防模块的至少一个安防单元上报的安防数据,包括:

[0047] 接收安防模块的至少一个安防单元通过MQTT(Message Queuing Telemetry Transport,消息队列遥测传输)中间件上报的安防数据,并将上报的所述安防数据经过封装处理之后,按照预设的插入规则插入待处理消息队列中。也即,在安防模块中,还包括MQTT中间件,安防模块中的各安防单元通过MQTT中间件连接所述物联网控制模块的所述接收单元;如此,上述安防模块的安防单元中的可以通过该MQTT中间件上报安防数据(除上述实施例中提及的安防数据之外,安防数据中还可以包括各安防单元对应的告警事件以及安防设备的状态信息等)。可理解地,在一实施例中,安防模块的至少一个安防单元通过MQTT中间件上报安防数据,并将安防数据经过处理封装后按照预设的插入规则(比如,按照处理完成的时间点的时间顺序进行排序或者按照数据类型排序)扔进Kafka消息队列(一个分布式的、高吞吐量、高可扩展性消息队列服务,也即待处理消息队列),之后,物联网控制模块从Kafka消息队列中提取封装之后的安防数据进行解析。

[0048] 在一实施例中,所述步骤S20中,所述根据接收到的所述安防数据确定告警事件,包括:

[0049] 自所述待处理消息队列中按照预设的解析顺序调取所述安防数据;在该步骤中,从Kafka消息队列中提取(提取顺序为预设的解析顺序,该顺序可以根据需求设定,亦可以根据提取指示中携带的解析顺序进行提取)封装之后的安防数据进行解析。

[0050] 解析所述安防数据的类型和数据值,并获取与所述安防数据的类型关联的告警阈值;在该步骤中,需要解析提取的安防数据的类型和数据值,随后获取与安防数据的类型关联的告警阈值,并将安防数据的类型关联的告警阈值与之前解析的安防数据的数据值进行

对比,以确定安防数据的数据值是否超过所述告警阈值,在并未超过时,认为该安防数据的数据值尚不构成告警事件,仅需要存储对应的安防数据即可。

[0051] 在一实施例中,所述解析所述安防数据的类型和数据值之后,还包括:获取与所述安防数据的类型关联的存储区域,将所述安防数据存储至与其关联的存储区域,并在存储完成之后接收反馈的处理完毕回执。在该实施例中,可以对各类安防数据在数据库中进行分类存储,且存储完后反馈一个回执消息以使得物联网控制模块获知该安防消息已经处理(存储)完毕。在所述安防数据的数据值超过所述告警阈值时,自与所述安防数据的类型关联的所有告警事件中,根据所述安防数据的数据值确认与所述安防数据对应的告警事件。也即,在安防数据的数据值超过所述告警阈值时,认为该安防数据已构成并触发告警事件,此时需要确认告警事件的属性,比如告警事件的类型等,以便于进一步根据告警事件的属性进行后续的联动处理。

[0052] 在一实施例中,所述根据所述安防数据的数据值确认与所述安防数据对应的告警事件之后,还包括:

[0053] 将与所述告警事件对应的安防数据进行封装处理之后插入告警队列中;也即,在确认该安防数据已构成并触发告警事件之后,会再次将安防数据进行封装后扔进一个告警队列中(该告警队列亦为Kafka消息队列)。

[0054] 在自所述告警队列中调取所述安防数据,并提取所述安防数据中与所述告警事件对应的所述安防设备的设备状态,将所述安防设备的设备状态存储在数据库中,同时将所述设备状态通过WebSocket(一种在单个TCP连接上进行全双工通信的协议)发送到决策模块进行实时显示,同时在所述决策模块中对与所述安防数据对应的所述告警事件进行警示。也即,自所述告警队列中获取到安防数据中与所述告警事件对应的所述安防设备的设备状态后,将设备状态存储在数据库中,同时将设备状态等信息通过WebSocket发送到决策模块进行实时显示,以使得可以通过上报的状态信息实现实时监控查看其各安防设备的当前运行状态。同时,本实施例还可以在决策模块中对该告警事件进行报警提示(可理解地,在物联网控制模块中对该告警事件进行单独报警提示亦可单独或者同步进行)。可理解地,物联网控制模块通过WebSocket的方式与决策模块进行消息传递,实现了决策模块对于安防模块的各安防单元的告警时间,设备状态,统计数据等的实时变化的掌控,可以使得决策模块真正做到对车站整个安防全貌的实时监控;并且,通过将安防数据放入待处理消息队列,并将与告警事件对应的安防数据放入告警队列中,按照一定顺序调取安防数据并进行对应处理,可以使并发的大量安防数据可以得到高效处理,提升了对整个安防系统的实时状态及告警的反应速度,使整个车站的所有运行都在掌控之中,可以避免出现意外。

[0055] 在一实施例中,所述步骤S30之后,也即所述根据所述预设联动规则,令需要联动的所述安防单元,控制对应的安防设备执行与其对应的联动事件之后,包括:

[0056] 获取各所述安防设备执行所述联动事件之后的执行结果,通过WebSocket将所述执行结果发送到决策模块进行实时显示,并根据所述执行结果调整与所述告警事件关联的所述预设联动规则。也即,物联网控制模块通过WebSocket的方式与决策模块进行消息传递,实现了决策模块对于安防模块的各安防单元的告警事件对应的联动事件的执行情况的实时变化的掌控,可以使得决策模块真正做到对车站整个安防全貌的实时监控。同时,根据联动事件的执行结果去调整预设联动规则,可以使得预设联动规则更适用于实际情况,使

得对于该告警事件的处理更为完善。

[0057] 在一实施例中,所述步骤S20中,所述调取与所述告警事件关联的预设联动规则之前,还包括:

[0058] 为所述预设联动规则分配对应的所述安防单元,并将所述安防单元与所述预设联动规则关联;具体地,为所述预设联动规则分配需要联动的所述安防单元,并将需要联动的所述安防单元的属性与所述预设联动规则关联;也即,在该实施例中,为预设联动规则配置需要联动的安防单元,且每一个预设联动规则中至少需要配置一个或一个以上需要联动的安防单元。所述安防单元的属性是指安防单元的名称、类型或唯一编码等可以代表该安防单元的属性。

[0059] 根据所述预设联动规则,为所述安防单元中对应的所述安防设备配置联动事件;具体地,为每一个需要联动的所述安防单元中需要联动的所述安防设备配置联动事件;联动事件是指一个安防设备在进行联动时需要执行的操作事件,比如,安防设备为出入口监控设备,所述联动事件可以是指所述出入口监控设备控制出入口的开关状态的切换。

[0060] 将每一项所述预设联动规则与至少一项告警事件关联。也即,对预设联动规则进行配置管理,还包括将其与告警事件关联,如此,在接收到该告警事件的触发指令时,可以直接根据该告警事件的属性调取该预设联动规则,进而通过该预设联动规则控制安防设备执行对应的联动事件。可理解地,在安防设备执行联动事件时,需要发送邮件信息(或以其他方式通知)通知给该安防设备的负责人,该安防设备需要执行的联动事件的相关信息。

[0061] 在一实施例中,所述安防数据处理方法还包括:

[0062] 接收登录用户发送的登录请求,自数据库中调取登录权限信息;所述登录权限信息中包括允许登录用户信息以及与每一项所述允许登录用户信息关联的允许登录区域;其中,所述允许登录用户信息是针对每一个注册用户预先设定的,该允许登录用户信息可以为该注册用户用于登录的账户信息,比如,一个注册用户允许被登录的账户的账号和密码。可理解地,所述登录权限信息中的每一个允许登录用户信息均与至少一个允许登录区域关联。若所述登录请求中包括的登录用户信息与所述允许登录用户信息匹配,根据所述允许登录用户信息关联的所述允许登录区域,对所述登录用户开放所述允许登录区域的访问权限。其中,所述登录用户信息是指当前进行登录的登录用户的账户信息(比如账号和密码)等。登录请求中包括的登录用户信息与所述允许登录用户信息匹配,可以是指登录用户当前用于登录的账号和密码,和与该登录用户对应的允许登录用户信息中的账号和密码一致。

[0063] 也即,在上述实施例中,用户可通过Web(World Wide Web,全球广域网)页面访问等访问方式去访问安防数据处理系统中的所有功能模块(比如安防模块、物联网控制模块、决策模块等),此时,需要用户首先登录安防数据处理系统,并且根据该登录用户的登录用户信息确定其访问和管理权限;如此,任何用户访问安防数据处理系统时,首先会对用户的权限进行检查,用户只可看到允许登录的功能模块中的被允许访问的页面或菜单(允许登录区域)。其中,登录权限信息等均被存储在数据库中。

[0064] 在一实施例中,所述安防数据处理方法还包括:

[0065] 接收车站展示指令,将车站的构造图以及所述车站中的所有车站安防设备以二维、三维形式中的至少一种展示在当前显示界面;也即,在该实施例中,可以通过二维或者

三维立体的形式一体化呈现车站安防全貌,将整个车站的设备及车站全貌展现出来,使运营人员实时掌握动态情况,对告警事件的发生地一目了然,方便他们快速响应并处理。车站展示指令可以在告警事件被触发时自动生成,亦可以由用户触发预设按钮之后生成。

[0066] 在一实施例中,所述安防数据处理方法还包括:

[0067] 接收包括安防设备的设备参数的设备配置指令,根据所述设备参数将所述安防设备配置至所述安防模块下的所述安防单元。也即,本实施例可以对安防模块中的各安防单元的安防设备的设备参数进行配置,设备参数包括设备类型、控制设备的命令、安防设备可以实现的设备状态、该安防设备所属的安防单元、设备安放的区域等进行管理配置,如此,可以方便后续将该安防设备对应的安防数据上报之后进行处理分析,也便于后续在进行设备新增或更换时提供参考价值。

[0068] 在一实施例中,如图2所示,提供一种安防数据处理系统,该安防数据处理系统与上述实施例中安防数据处理方法一一对应。该安防数据处理系统包括安防模块2和与所述安防模块2通信连接的物联网控制模块1,所述安防模块2包括至少一个安防单元,每一个所述安防单元包括至少一个安防设备;

[0069] 所述物联网控制模块1包括:

[0070] 接收单元101,用于接收安防模块的至少一个安防单元上报的安防数据,其中,每一个所述安防单元包括至少一个安防设备;

[0071] 调取单元102,用于根据接收到的所述安防数据确定告警事件,调取与所述告警事件关联的预设联动规则;

[0072] 执行单元103,用于根据所述预设联动规则,令需要联动的所述安防单元,控制对应的安防设备执行与其对应的联动事件。

[0073] 本发明的安防数据处理系统中包括通信连接的安防模块和物联网控制模块,且不同用途的安防单元均集成在安防模块中,如此,可以在物联网控制模块中对不同用途的安防单元的安防数据进行统一处理,并通过综合处理安防数据确定告警事件并按照预设联动规则对该告警事件进行处理;如此,一方面,对不同用途的安防单元的安防数据进行统一处理,使得整个车站的安防运行状态更为清晰,可以令车站运营人员更清楚地了解整个车站的安防运行状态,进而可以对各种告警及紧急事件及时进行分析评估处理,这对整个车站的安防工作有很大的帮助和提升;另一方面,通过综合处理安防数据确定告警事件并按照预设联动规则对该告警事件进行处理,可以调动整个车站的各安防单元的安防设备联动执行与其对应的所述联动事件,大大提升了车站对于告警事件的处理效率,使告警事件可以得到及时控制和稳妥处理,保证了车站的安全高效运行。

[0074] 在一实施例中,所述安防单元包括视频监控单元21、入侵监控单元22、出入口监控单元23、安检单元24和电子巡检单元25中的至少一种;在一实施例中,如图3所示,所述安防模块2中的安防单元包括视频监控单元21、入侵监控单元22、出入口监控单元23、安检单元24和电子巡检单元25。

[0075] 所述安防数据包括以下数据中的至少一种:

[0076] 所述视频监控单元21根据预设的布防信息,对摄像设备拍摄的视频信息进行分析之后获取的视频监控数据;

[0077] 所述入侵监控单元22的入侵监控设备,对车站的预设禁止区域的入侵监控数据;

- [0078] 所述出入口监控单元23的出入口监控设备,对车站出入口进行监控的通行数据;
- [0079] 所述安检单元24的安检设备,对车站进行安检的安检数据,所述安检数据包括安检图像或/和危险品检测信息;
- [0080] 所述电子巡检单元25的巡检设备,根据巡检计划中的各巡检点的巡检路线,进行巡检之后的巡检数据。
- [0081] 在一实施例中,如图4所示,所述安防模块2通过MQTT中间件连接所述物联网控制模块1的所述接收单元101;
- [0082] 所述接收单元101包括:
- [0083] 处理子单元1011,用于接收安防模块2的至少一个安防单元通过MQTT中间件上报的安防数据,并将上报的所述安防数据经过封装处理之后,按照预设的插入规则插入待处理消息队列中。
- [0084] 在一实施例中,如图5所示,所述调取单元102包括:
- [0085] 调取子单元1021,自所述待处理消息队列中按照预设的解析顺序调取所述安防数据;
- [0086] 解析子单元1022,用于解析所述安防数据的类型和数据值,并获取与所述安防数据的类型关联的告警阈值;
- [0087] 确认子单元1023,用于在所述安防数据的数据值超过所述告警阈值时,根据所述安防数据的数据值确认与所述安防数据对应的告警事件。
- [0088] 在一实施例中,如图6所示,所述安防数据处理系统还包括与所述物联网控制模块1通信连接的决策模块3;
- [0089] 所述调取单元102还包括:
- [0090] 发送子单元1024,用于将与所述安防数据对应的告警事件插入告警队列中,记录与所述告警事件对应的所述安防设备的设备状态,并将所述设备状态通过WebSocket发送到决策模块进行实时显示,同时在所述决策模块中对与所述安防数据对应的所述告警事件进行警示。
- [0091] 在一实施例中,如图7所示,所述物联网控制模块1还包括:
- [0092] 调整单元104,用于获取各所述安防设备执行所述联动事件之后的执行结果,通过WebSocket将所述执行结果发送到决策模块进行实时显示,并根据所述执行结果调整与所述告警事件关联的所述预设联动规则。
- [0093] 在一实施例中,如图8所示,所述调取单元102还包括:
- [0094] 存储子单元1025,用于获取与所述安防数据的类型关联的存储区域,将所述安防数据存储至与其关联的存储区域,并在存储完成之后接收反馈的处理完毕回执。
- [0095] 在一实施例中,如图9所示,所述物联网控制模块1还包括:
- [0096] 分配单元105,用于为所述预设联动规则分配对应的所述安防单元,并将所述安防单元与所述预设联动规则关联;
- [0097] 联动事件配置单元106,用于根据所述预设联动规则,为所述安防单元中对应的所述安防设备配置联动事件;
- [0098] 关联单元107,用于将每一项所述预设联动规则与至少一项告警事件关联。
- [0099] 在一实施例中,如图10所示,所述物联网控制模块1还包括:

[0100] 登录模块108,用于接收登录用户发送的登录请求,自数据库中调取登录权限信息;所述登录权限信息中包括允许登录用户信息以及与每一项所述允许登录用户信息关联的允许登录区域;

[0101] 权限验证模块109,用于若所述登录请求中包括的登录用户信息与所述允许登录用户信息匹配,根据所述允许登录用户信息关联的所述允许登录区域,对所述登录用户开放所述允许登录区域的访问权限。

[0102] 在一实施例中,如图11所示,所述物联网控制模块1还包括:

[0103] 展示模块110,用于接收车站展示指令,将车站的构造图以及所述车站中的所有车站安防设备以二维、三维形式中的至少一种展示在当前显示界面。

[0104] 在一实施例中,如图11所示,所述物联网控制模块1还包括:

[0105] 设备配置模块111,用于接收包括安防设备的设备参数的设备配置指令,根据所述设备参数将所述安防设备配置至所述安防模块下的所述安防单元。

[0106] 关于安防数据处理系统的具体说明可以参见上文中对于安防数据处理方法的说明,在此不再赘述。上述安防数据处理系统中的各个模块可全部或部分通过软件、硬件及其组合来实现。上述各模块可以硬件形式内嵌于或独立于计算机设备中的处理器中,也可以以软件形式存储于计算机设备中的存储器中,以便于处理器调用执行以上各个模块对应的操作。

[0107] 在一个实施例中,本发明的安防数据处理系统为一个智慧车站的安防数据处理系统,集成了各个安防单元,可以同时将各个不同安防单元的数据进行统一处理显示,并将各种告警事件及其他信息按照预设联动规则联动处理,使得运营人员清楚的了解整个车站的安防运行状态,对各种告警及紧急事件及时进行分析评估处理,这对整个车站的安防工作有很大的帮助和提升。在本实施例中,如图12所示,可以将该智慧车站的安防数据处理系统分为三个层次:决策层4、业务模块层5和支持层6;其中,决策层4至少包括上述实施例中的决策模块3,决策层4主要用于进行告警分析(评估是否构成告警事件)和紧急事件的评估(评估告警事件的紧急等级并进行不同分级处理),可理解地,决策层4还用于对其他事件进行决策(比如指示某个安防单元执行某个安防措施)或者显示(比如显示执行所述联动事件之后执行结果或与所述告警事件对应的所述安防设备的设备状态等)。

[0108] 业务模块层5主要根据决策层的对于告警事件的告警分析或者紧急事件的评估的最终决策去指示支持层执行联动事件,或根据决策层的决策指示支持层执行其他待执行事件。业务模块层5包括:

[0109] 安防模块2中的所有安防单元:图12中所示的实施例中,安防单元包括视频监控单元21、入侵监控单元22、出入口监控单元23、安检单元24和电子巡检单元25。其中,视频监控单元21根据预设的布防信息,对摄像设备拍摄的视频信息进行分析之后获取视频监控数据。入侵监控单元22通过入侵监控设备获取对车站的预设禁止区域的入侵监控数据。出入口监控单元23通过出入口监控设备获取对车站出入口进行监控的通行数据。安检单元24通过安检设备获取对车站进行安检的安检数据,所述安检数据包括安检图像或/和危险品检测信息。电子巡检单元25通过巡检设备,获取根据巡检计划中的各巡检点的巡检路线进行巡检之后的巡检数据。

[0110] 接收单元101,用于接收安防模块的至少一个安防单元上报的安防数据,其中,每

一个所述安防单元包括至少一个安防设备。

[0111] 调取单元102,用于根据接收到的所述安防数据确定告警事件,调取与所述告警事件关联的预设联动规则。

[0112] 执行单元103,用于根据所述预设联动规则,令需要联动的所述安防单元,控制对应的安防设备执行与其对应的联动事件。

[0113] 展示模块110,用于接收车站展示指令,将车站的构造图以及所述车站中的所有车站安防设备以二维、三维形式中的至少一种展示在当前显示界面。

[0114] 支持层6主要包括:

[0115] 各安防单元的安防设备61;其中,安防设备61包括上述视频监控单元21的摄像设备、入侵监控单元22的入侵监控设备、出入口监控单元23的入口监控设备、安检单元24的安检设备和电子巡检单元25巡检设备。

[0116] 分配单元105,用于为所述预设联动规则分配对应的所述安防单元,并将所述安防单元与所述预设联动规则关联。

[0117] 联动事件配置单元106,用于根据所述预设联动规则,为所述安防单元中对应的所述安防设备配置联动事件。

[0118] 关联单元107,用于将每一项所述预设联动规则与至少一项告警事件关联。

[0119] 登录模块108,用于接收登录用户发送的登录请求,自数据库中调取登录权限信息;所述登录权限信息中包括允许登录用户信息以及与每一项所述允许登录用户信息关联的允许登录区域。

[0120] 权限验证模块109,用于若所述登录请求中包括的登录用户信息与所述允许登录用户信息匹配,根据所述允许登录用户信息关联的所述允许登录区域,对所述登录用户开放所述允许登录区域的访问权限。

[0121] 设备配置模块111,用于接收包括安防设备的设备参数的设备配置指令,根据所述设备参数将所述安防设备配置至所述安防模块下的所述安防单元。

[0122] 在一个实施例中,如图13所示,本发明的安防数据处理系统为一个智慧车站的安防数据处理系统,该系统主要包括UI (User Interface:用户界面) 应用层7、物联网平台8、安防模块2和数据库9四个部分。其中:

[0123] UI应用层7:用户可通过Web页面访问该UI应用层7中的所有功能模块。如图13所示的UI应用层7中主要包括决策模块3以及物联网控制模块1中的部分功能模块,如图13中所示的实施例中,UI应用层7具体包括的功能模块如下:

[0124] 决策模块3:用于进行告警分析(评估是否构成告警事件)和紧急事件的评估(评估告警事件的紧急等级并进行不同分级处理),可理解地,还用于对其他事件进行决策(比如指示某个安防单元执行某个安防措施)或者显示物联网平台8上报的执行所述联动事件之后执行结果或与所述告警事件对应的所述安防设备的设备状态等,以供实现随时实时进行监控车站状态。

[0125] 展示模块110,用于接收车站展示指令,将车站的构造图以及所述车站中的所有车站安防设备以二维、三维形式中的至少一种展示在当前显示界面。

[0126] 登录模块108,用于接收登录用户发送的登录请求,自数据库中调取登录权限信息;所述登录权限信息中包括允许登录用户信息以及与每一项所述允许登录用户信息关联

的允许登录区域。

[0127] 权限验证模块109,用于若所述登录请求中包括的登录用户信息与所述允许登录用户信息匹配,根据所述允许登录用户信息关联的所述允许登录区域,对所述登录用户开放所述允许登录区域的访问权限。

[0128] 物联网平台8:通过WebSocket的方式与UI应用层7进行消息传递,实现了系统的告警,状态,统计等的实时变化,真正做到对车站整个安防全貌的实时监控。物联网平台8主要包括物联网控制模块1中的部分功能模块,如图13中所示的实施例,物联网平台8具体包括的功能模块如下:

[0129] 设备配置模块111:用于接收包括安防设备的设备参数的设备配置指令,根据所述设备参数将所述安防设备配置至所述安防模块下的所述安防单元。也即,对添加到物联网平台201上的各设备(比如安防设备)的类型,参数以及命令等各种功能进行管理配置,方便后续设备上报数据处理分析,以及以后车站安防单元设备新增或更换。

[0130] 接收单元101,用于接收安防模块的至少一个安防单元上报的安防数据,其中,每一个所述安防单元包括至少一个安防设备。

[0131] 调取单元102,用于根据接收到的所述安防数据确定告警事件,调取与所述告警事件关联的预设联动规则;

[0132] 执行单元103,用于根据所述预设联动规则,令需要联动的所述安防单元,控制对应的安防设备执行与其对应的联动事件。

[0133] 调整单元104,用于获取各所述安防设备执行所述联动事件之后的执行结果,通过WebSocket将所述执行结果发送到决策模块进行实时显示,并根据所述执行结果调整与所述告警事件关联的所述预设联动规则。

[0134] 分配单元105,用于为所述预设联动规则分配对应的所述安防单元,并将所述安防单元与所述预设联动规则关联;

[0135] 联动事件配置单元106,用于根据所述预设联动规则,为所述安防单元中对应的所述安防设备配置联动事件;

[0136] 关联单元107,用于将每一项所述预设联动规则与至少一项告警事件关联。

[0137] 如图14所示,在一实施例中,物联网平台8对安防数据进行处理的具体过程如下: Event Source20232通过MQTT中间件(MQTT20231)获取上报的安防数据(包括告警事件或其他事件等),将安防数据经过处理封装后扔进待处理消息队列(Kafka消息队列)中, Inbound Processing20233再从待处理消息队列接收到安防数据进行解析,通过Event Management20234对各种事件在数据库9中进行分类存储,存储完后通过Kafka给Inbound Processing20233回执消息告诉它已处理完;同时如果是告警或者遥测值(安防数据的数据值)超过告警阈值,触发Linkage Engine20235,进行联动处理。同时Inbound Processing20233会再次将安防数据对应的告警事件进行封装扔进告警队列(Kafka消息队列), Device State20236通过Kafka获取到安防数据对应的告警事件后将设备状态存储在数据库9,同时将设备状态等信息通过WebSocket20237发送到UI应用层7进行实时显示,以及报警提示。本实施例中,可以对并发的大量数据进行高效处理,提升了系统对整个安防系统的实时状态及告警的反应速度,使整个车站的所有运行都在掌控之中,防止出现意外。

[0138] 安防模块2:图13中所示的实施例,安防模块2中的所有安防单元包括视频监控单

元21、入侵监控单元22、出入口监控单元23、安检单元24和电子巡检单元25。其中,视频监控单元21根据预设的布防信息,对摄像设备拍摄的视频信息进行分析之后获取视频监控数据。入侵监控单元22通过入侵监控设备获取对车站的预设禁止区域的入侵监控数据。出入口监控单元23通过出入口监控设备获取对车站出入口进行监控的通行数据。安检单元24通过安检设备获取对车站进行安检的安检数据,所述安检数据包括安检图像或/和危险品检测信息。电子巡检单元25通过巡检设备,获取根据巡检计划中的各巡检点的巡检路线进行巡检之后的巡检数据。参照本发明中的安防数据处理方法中所述,各安防单元除了通过接口进行数据获取外,各个安防单元的安防设备上报事件及告警时会通过MQTT消息中间件上报至物联网平台8。

[0139] 数据库9:保存安防数据处理系统需要保存的所有数据。如图14所示,所述数据库9可以为以下类型数据库:MongoDB、MySQL、InfluxDB。

[0140] 在一个实施例中,提供了一种计算机设备,该计算机设备可以是服务器,其内部结构图可以如图15所示。该计算机设备包括通过系统总线连接的处理器、存储器、网络接口和数据库。其中,该计算机设备的处理器用于提供计算和控制能力。该计算机设备的存储器包括非易失性存储介质、内存储器。该非易失性存储介质存储有操作系统、计算机可读指令和数据库。该内存储器为非易失性存储介质中的操作系统和计算机可读指令的运行提供环境。该计算机可读指令被处理器执行时以实现上述的方法。

[0141] 在一个实施例中,提供了一种计算机设备,包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机可读指令,处理器执行计算机可读指令时实现以下步骤:

[0142] 接收安防模块的至少一个安防单元上报的安防数据;每一个所述安防单元包括至少一个安防设备;

[0143] 根据接收到的所述安防数据确定告警事件,调取与所述告警事件关联的预设联动规则;所述预设联动规则中包括所有需要联动的所述安防单元的属性以及需要联动的所述安防单元中的所有需要联动的所述安防设备的待执行的联动事件;

[0144] 令需要联动的所述安防单元指示该安防单元中需要联动的各所述安防设备执行与其对应的所述联动事件。

[0145] 在一个实施例中,提供了一种计算机可读存储介质,其上存储有计算机可读指令,计算机可读指令被处理器执行时实现上述的方法。

[0146] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程,是可以通过计算机可读指令来指令相关的硬件来完成,所述的计算机可读指令可存储于一非易失性计算机可读存储介质中,该计算机可读指令在执行时,可包括如上述各方法的实施例的流程。其中,本发明所提供的各实施例中所使用的对存储器、存储、数据库或其它介质的任何引用,均可包括非易失性和/或易失性存储器。非易失性存储器可包括只读存储器(ROM)、可编程ROM(PROM)、电可编程ROM(EPROM)、电可擦除可编程ROM(EEPROM)或闪存。易失性存储器可包括随机存取存储器(RAM)或者外部高速缓冲存储器。作为说明而非局限,RAM以多种形式可得,诸如静态RAM(SRAM)、动态RAM(DRAM)、同步DRAM(SDRAM)、双数据率SDRAM(DDRSDRAM)、增强型SDRAM(ESDRAM)、同步链路DRAM(SLDRAM)、存储器总线直接RAM(RDRAM)、直接存储器总线动态RAM(DRDRAM)、以及存储器总线动态RAM(RDRAM)等。

[0147] 所属领域的技术人员可以清楚地了解到,为了描述的方便和简洁,仅以上述各功

能单元或模块的划分进行举例说明,实际应用中,可以根据需要而将上述功能分配由不同的功能单元或模块完成,即将所述系统的内部结构划分成不同的功能单元或模块,以完成以上描述的全部或者部分功能。

[0148] 以上所述实施例仅用以说明本发明的技术方案,而非对其限制;尽管参照前述实施例对本发明进行了详细的说明,本领域的普通技术人员应当理解:其依然可以对前述各实施例所记载的技术方案进行修改,或者对其中部分技术特征进行等同替换;而这些修改或者替换,并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围,均应包含在本发明的保护范围之内。

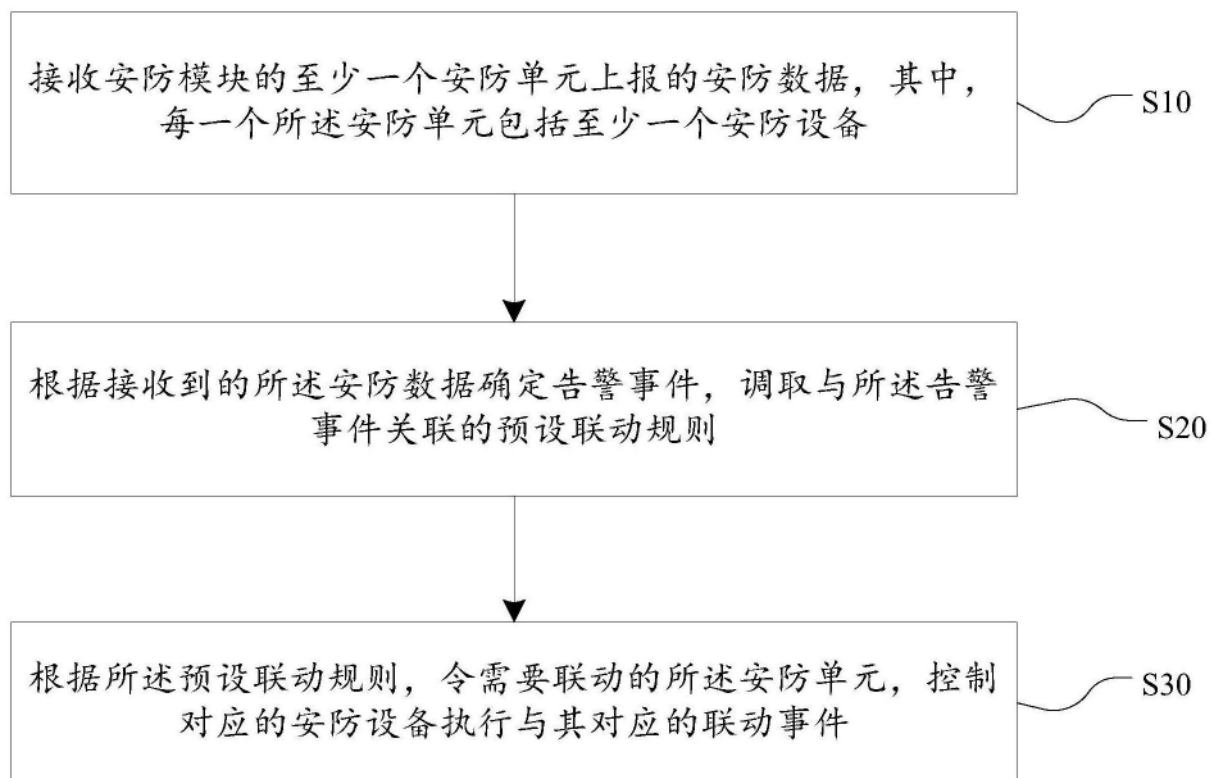


图1

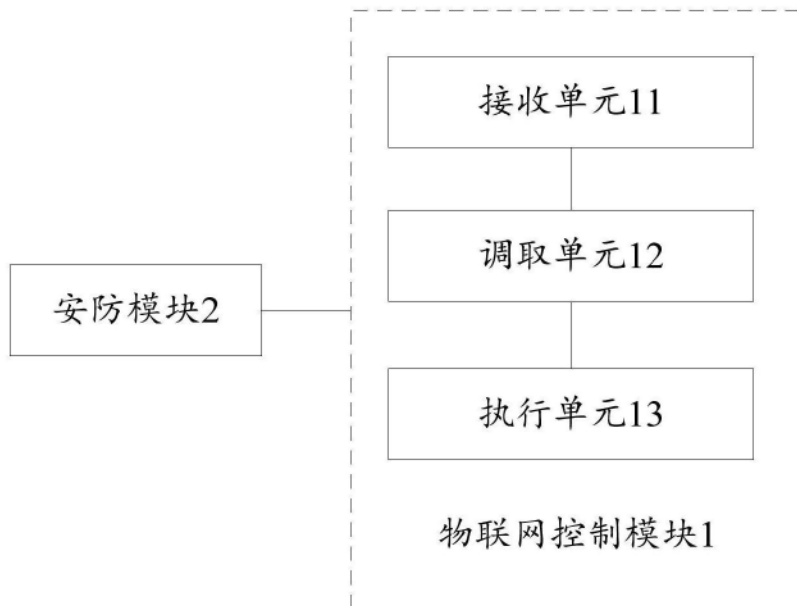


图2

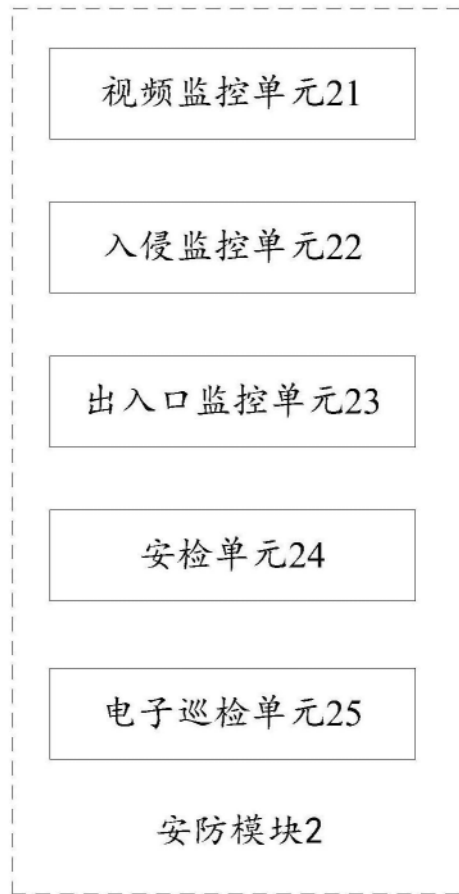


图3

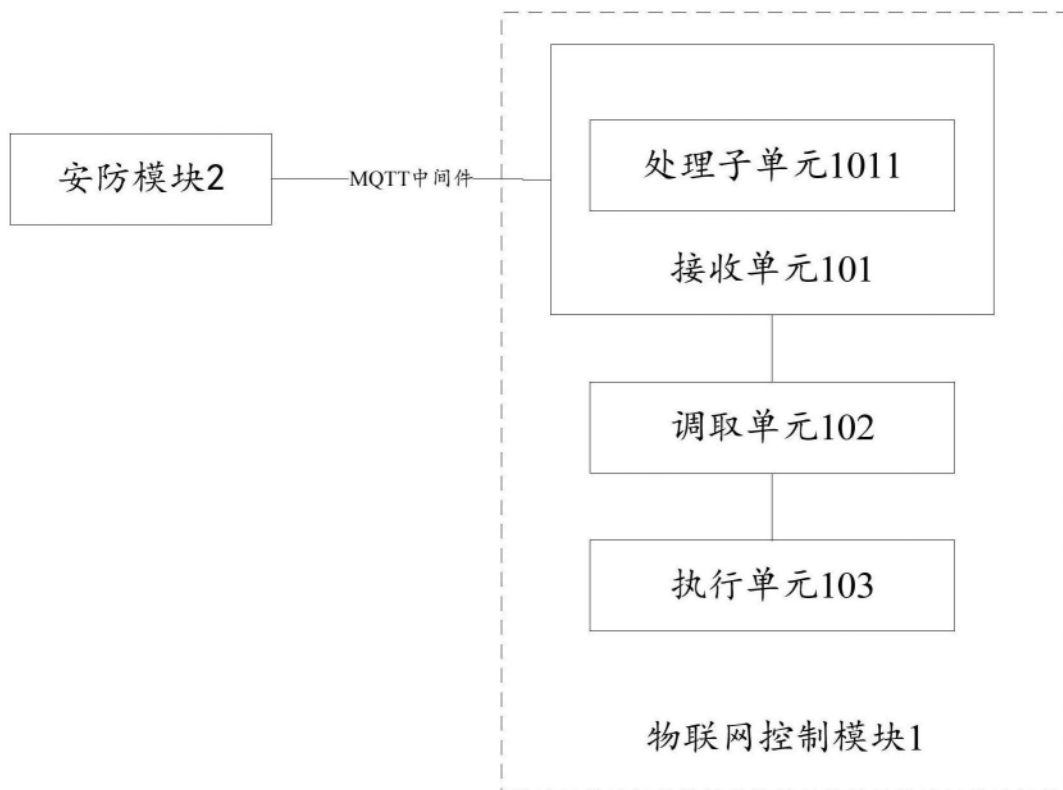


图4



图5

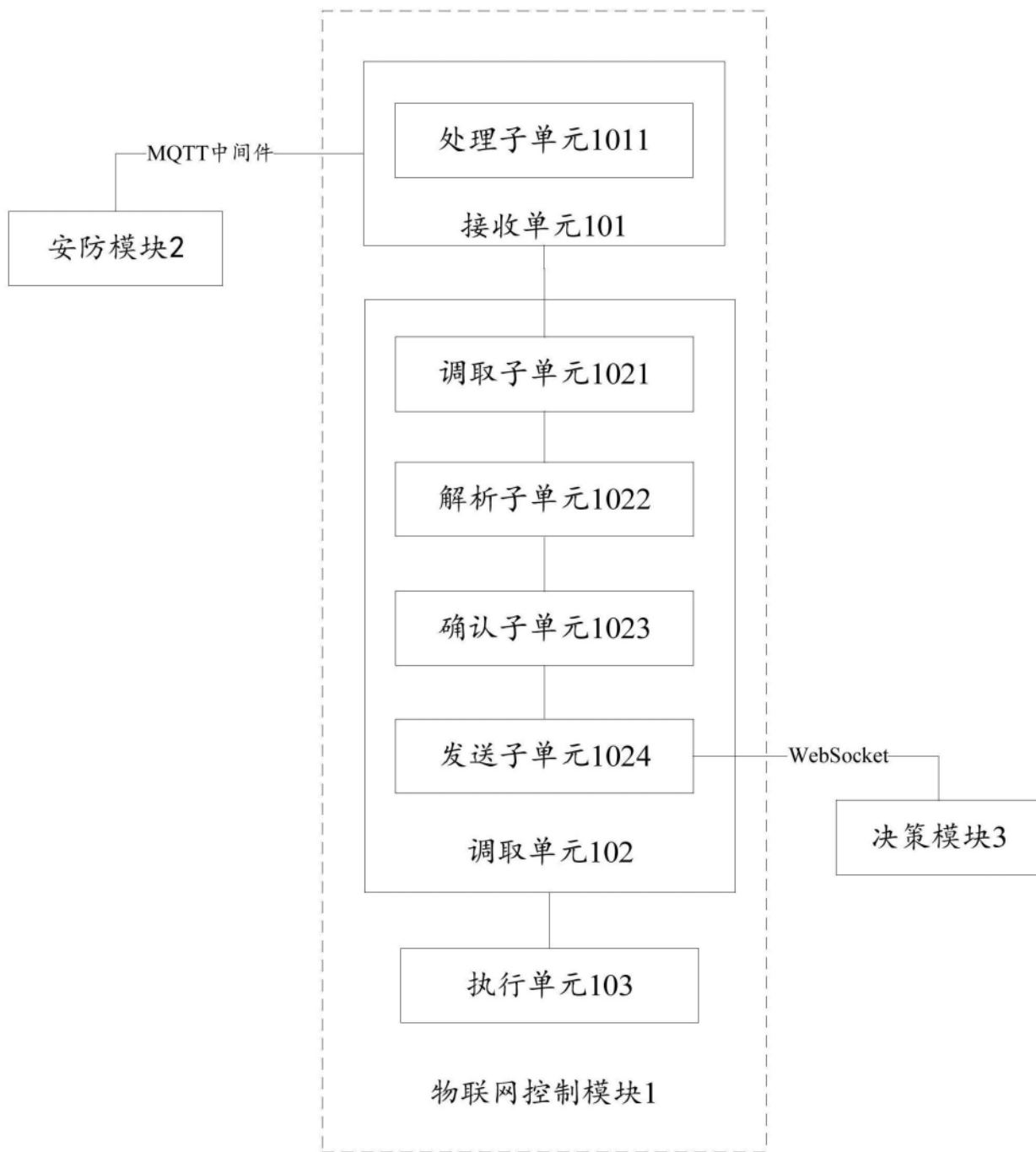


图6

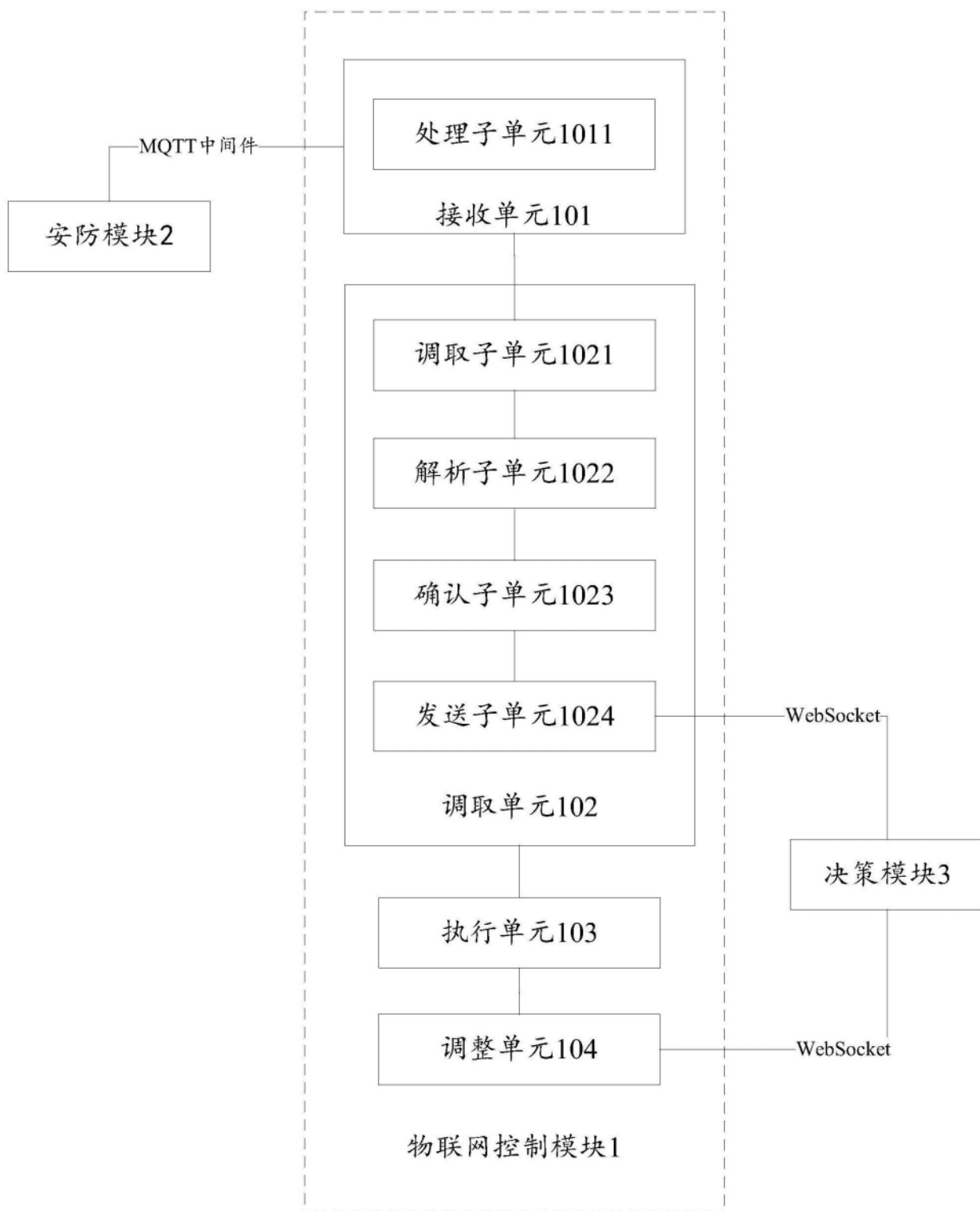


图7

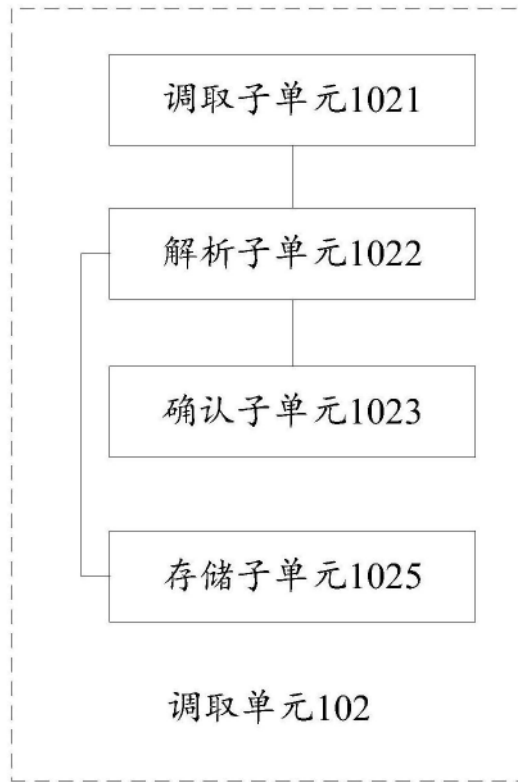


图8

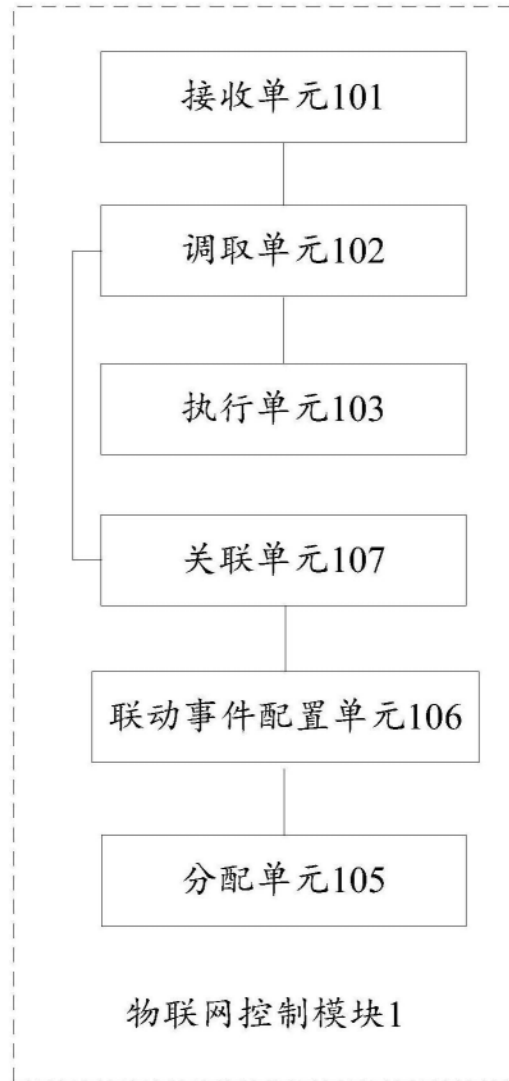


图9



图10



图11

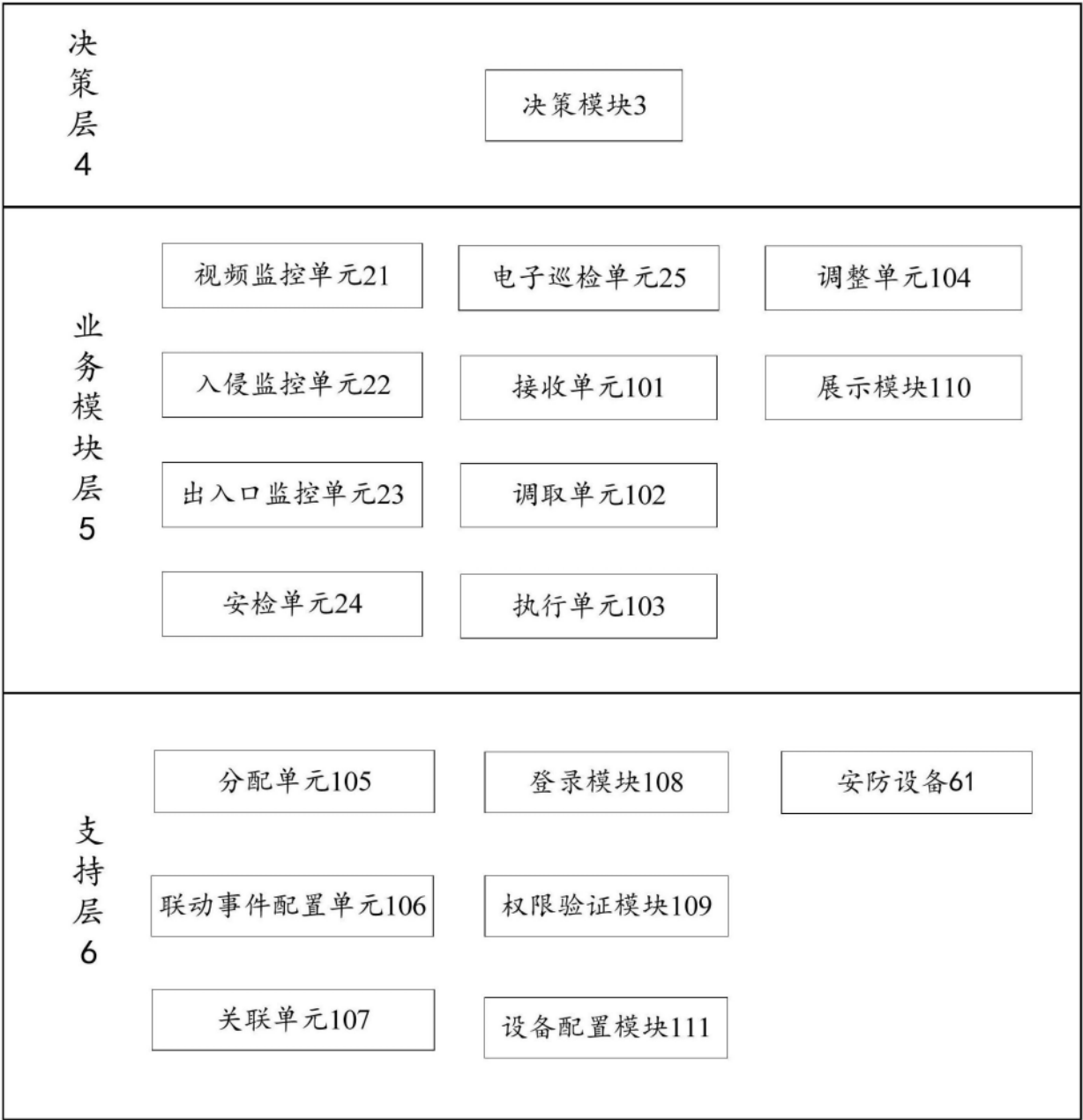


图12

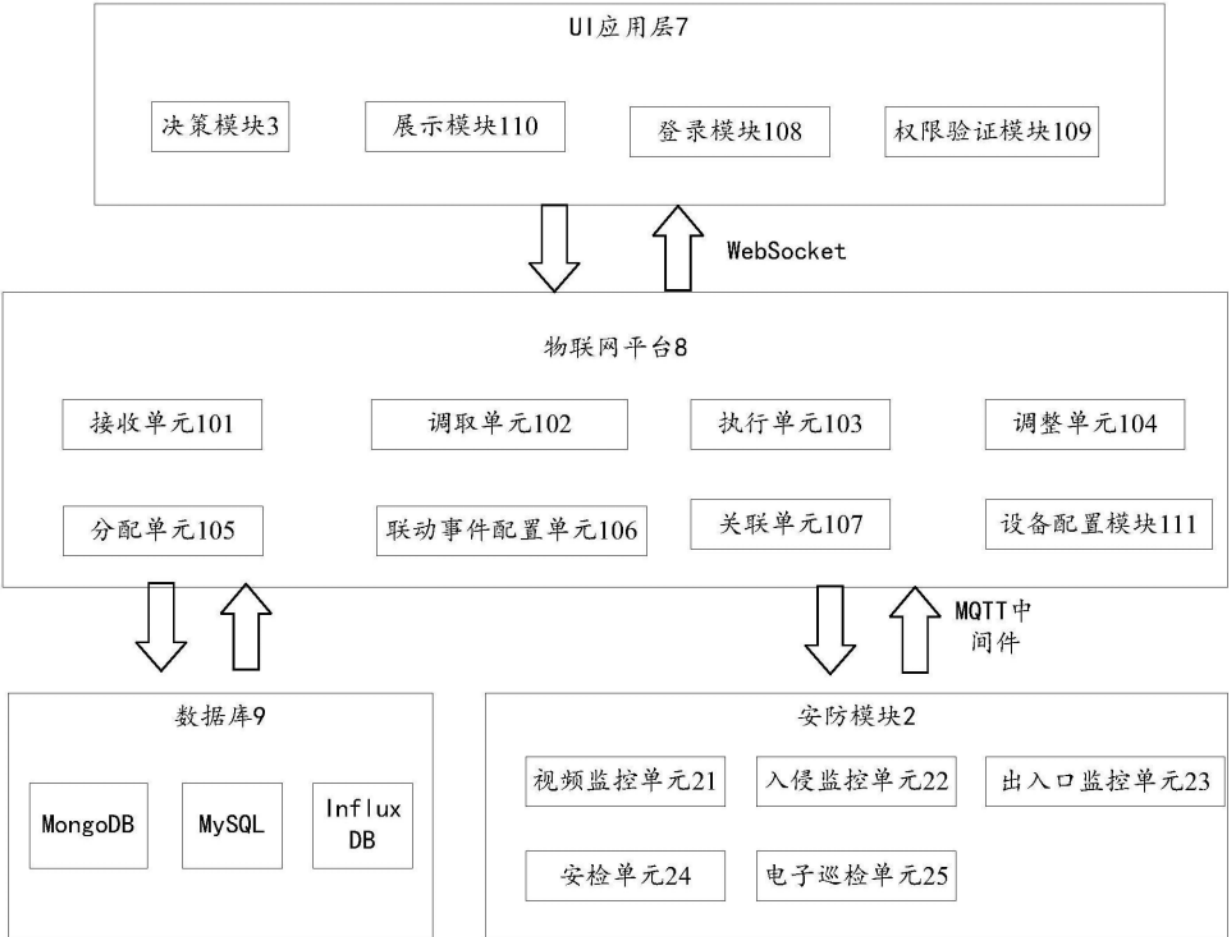


图13

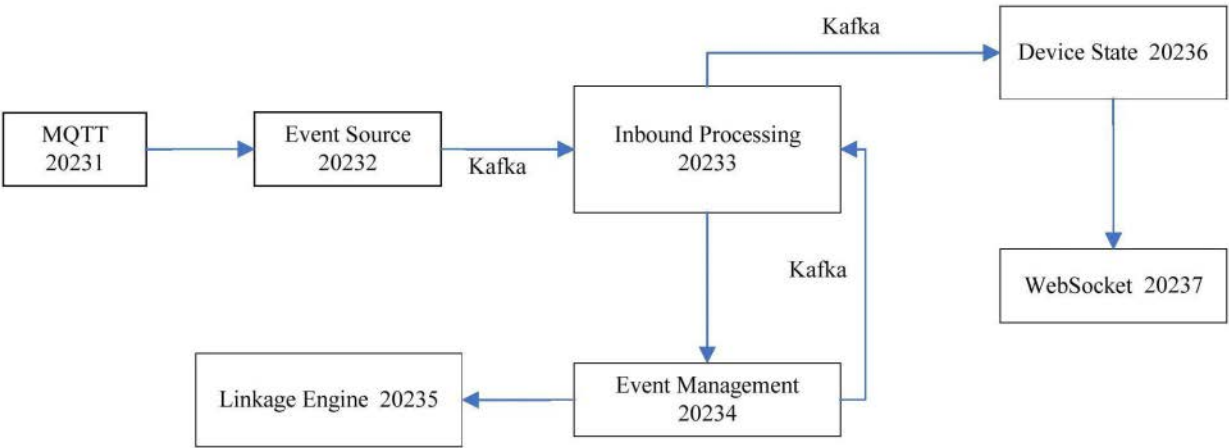


图14

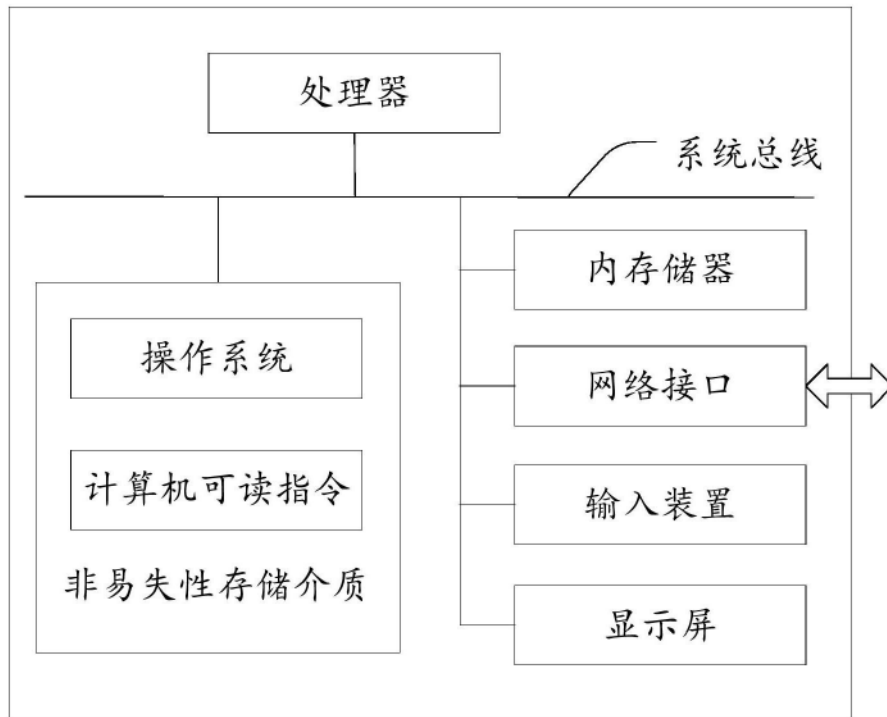


图15