(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 103459234 B
(45)授权公告日 2016.07.06

(21)申请号 201280017183.7
(22)申请日 2012.03.28
(30)优先权数据
102011006772.8 2011.04.05 DE
(85)PCT国际申请进入国家阶段日
2013.10.08
(86)PCT国际申请的申请数据
PCT/EP2012/055460 2012.03.28
(87)PCT国际申请的公布数据
WO2012/136525 DE 2012.10.11
(73)专利权人 西门子公司
地址 德国慕尼黑
(72)发明人 R. 法尔克 S. 弗里斯
(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 宣力伟 杨国治
(51)Int.Cl.
B61L 15/00(2006.01)
B61L 27/00(2006.01)
(56)对比文件
DE 102007041177 A1,2009.03.05,
CN 101391616 A,2009.03.25,
CN 101722971 A,2010.06.09,
审查员 郑勇龙

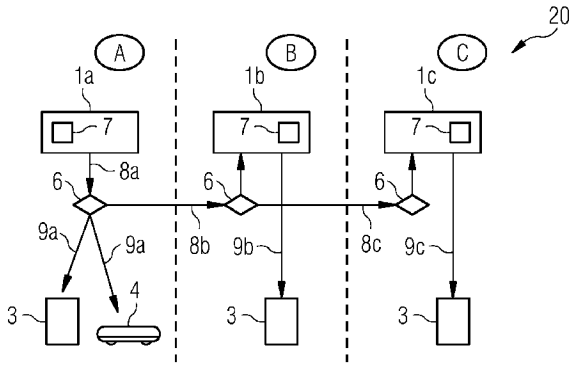
权利要求书2页 说明书6页 附图4页

(54)发明名称

用于列车安全系统的密钥管理的系统和方法

(57)摘要

本发明涉及一种用于分配用来对轨道车辆安全系统的交通引导信息进行加密的通讯密钥(6)的方法,具有以下步骤,根据轨道车辆(4)的所计划的行驶路线在第一路段运营商的第一加密管理中心(1a)中生成通讯密钥(6),将通讯密钥(6)提供给第二路段运营商的第二加密管理中心(1b),将通讯密钥(6)提供给通过第一加密管理中心的轨道车辆(4),并且用通讯密钥(6)对轨道车辆(4)的交通引导信息进行加密,使得轨道车辆(4)与第一路段运营商的路段中心(3)以及第二路段运营商的路段中心(3)防止被操纵地进行通讯。



CN 103459234 B

1.用于分配用来对轨道车辆安全系统的交通引导信息进行加密的通讯密钥(6;6a、6b、6c;11)的方法,其特征在于,所述方法具有以下步骤:

根据轨道车辆(4)的计划的行驶路线在第一路段运营商的第一加密管理中心(1a)中生成通讯密钥(6;6a、6b、6c;11);

将所述通讯密钥(6;6a、6b、6c;11)提供给第二路段运营商的第二加密管理中心(1b);

通过所述第一加密管理中心将所述通讯密钥(6;6a、6b、6c;11)提供给所述轨道车辆(4);并且

借助所述通讯密钥(6;6a、6b、6c;11)对所述轨道车辆(4)的交通引导信息进行加密,用于使所述轨道车辆(4)与第一路段运营商的路段中心(3)以及第二路段运营商的路段中心(3)防止被操纵地进行通讯,

其中在控制所述第一加密管理中心(1a)的情况下进行通讯密钥的生成和分配,并且所述第二加密管理中心(1b)取决于通过所述第一加密管理中心(1a)进行的控制。

2.按权利要求1所述的方法,还具有以下步骤:

通过所述第一路段运营商将所述通讯密钥(6;6a、6b、6c;11)提供给所述第一路段中心(2a;3);并且

通过所述第二路段运营商将所述通讯密钥(6;6a、6b、6c;11)提供给所述第二路段中心(2b;3)。

3.按权利要求2所述的方法,其中,所述通讯密钥包括多个路段中心所特有的通讯密钥(6a、6b、6c),其中将所述通讯密钥(6;6a、6b、6c;11)提供给所述第二加密管理中心(1b)包括,将一组路段中心所特有的通讯密钥(6a、6b、6c)提供给所述第二加密管理中心(1b),所述一组路段中心所特有的通讯密钥配属于所述第二路段运营商的第二路段中心(2b;3)。

4.按权利要求3所述的方法,其中,在第一加密管理中心(1a)中生成所述通讯密钥(6;6a、6b、6c;11)包括,通过密钥求导方法从主通讯密钥(6)中导出所述路段中心所特有的通讯密钥(6a、6b、6c)。

5.按权利要求4所述的方法,其中执行,从所述轨道车辆(4)的控制计算机中导出所述路段中心所特有的通讯密钥(6a、6b、6c)。

6.按权利要求4所述的方法,其中执行,从所述第一以及第二加密管理中心(1a、1b)中导出所述路段中心所特有的通讯密钥(6a、6b、6c)。

7.按权利要求6所述的方法,其中执行,通过仅仅用于所述第一路段中心(2a;3)的所述第一加密管理中心(1a)导出所述路段中心所特有的通讯密钥(6a、6b、6c)并且通过仅仅用于第二路段中心(2b;3)的第二加密管理中心(1b)导出所述路段中心所特有的通讯密钥(6a、6b、6c)。

8.按权利要求2所述的方法,其中,所述通讯密钥包括多个轨道车辆所特有的通讯密钥(6a、6b、6c),其中将所述通讯密钥(6;6a、6b、6c;11)提供给轨道车辆(4)包括,从所述多个轨道车辆所特有的通讯密钥(11)中提供对于所述轨道车辆(4)而言特有的通讯密钥。

9.按权利要求8所述的方法,此外还具有以下步骤:

从多个轨道车辆所特有的通讯密钥(6a、6b、6c)中分别导出多个路段中心所特有的通讯密钥(11);并且

将多个路段中心所特有的通讯密钥(11)中的一组路段中心所特有的通讯密钥(11)提

供给所述第二加密管理中心(1b),所述路段中心所特有的通讯密钥对于轨道车辆特有地配属于第二路段运营商的第二路段中心(2b;3)。

10.按权利要求9所述的方法,其中执行,通过所述轨道车辆(4)的控制计算机从所述多个轨道车辆所特有的通讯密钥(6a、6b、6c)中导出所述多个路段中心所特有的通讯密钥(11)。

11.按权利要求1到10中任一项所述的方法,其中,由用于调度控制的引导系统提供所述轨道车辆(4)的计划的行驶路线,并且其中所述第一加密管理中心(1a)自动地执行生成和提供所述通讯密钥(6;6a、6b、6c;11)。

12.控制装置(7),在第一轨道网络路段运营商的第一加密管理中心(1a)中,用于分配用来对轨道车辆安全系统的交通引导信息进行加密的通讯密钥(6;6a、6b、6c;11),其特征在于,所述控制装置具有:

生成装置,所述生成装置设置用于根据轨道车辆(4)的计划的行驶路线生成通讯密钥(6;6a、6b、6c;11);以及

提供装置,所述提供装置设置用于将所生成的通讯密钥(6;6a、6b、6c;11)提供给第二路段运营商的第二加密管理中心(1b)和所述轨道车辆(4),其中用于对所述轨道车辆(4)的交通引导信息进行加密的通讯密钥(6;6a、6b、6c;11)设置用于使所述轨道车辆(4)与第一路段运营商的路段中心(2a;3)以及第二路段运营商的运营中心(2b;3)防止被操纵地进行通讯,

其中在控制所述第一加密管理中心(1a)的情况下进行通讯密钥的生成和分配,并且所述第二加密管理中心(1b)取决于通过所述第一加密管理中心(1a)进行的控制。

13.轨道车辆安全系统(20;30;40;50),其特征在于,所述轨道车辆安全系统具有:

按权利要求12所述的控制装置(7);

第一加密管理中心(1a),在所述第一加密管理中心中布置有控制装置(7);

多个第一路段中心(2a;3),所述第一路段中心设置用于,由所述第一加密管理中心(1a)提供由所述控制装置(7)生成的用于对轨道车辆的交通引导信息进行加密的通讯密钥(6;6a、6b、6c;11);

第二加密管理中心(1b);以及

多个第二路段中心(2b;3),所述第二路段中心设置用于,由所述第二加密管理中心(1b)提供由所述控制装置(7)生成的用于对轨道车辆(4)的交通引导信息进行加密的通讯密钥(6;6a、6b、6c;11)。

用于列车安全系统的密钥管理的系统和方法

技术领域

[0001] 本发明涉及一种用于列车安全系统的密钥管理的系统和方法。

背景技术

[0002] 在轨道交通中用于列车安全的安全系统是所谓的欧洲列车控制系统(“ETCS”,European Train Control System)。所述交通引导系统通常利用无线电数据传递、例如通过GSM-R在轨道机动车或者其列车安全计算机、例如欧洲重要计算机和静态的路段中心、无线闭塞中心(“RBC”,Radio Block Centres)之间交换引导信息和安全消息。为了在传递时保护数据防止无意的运营以及传递失误,用加密的校验和保护数据,对于该校验和的计算和/或核实而言需要加密的密钥。

[0003] 通常使用对称的加密方法,使得不仅所述轨道机动车而且所述路段中心都必须具有至少一个密钥。因为轨道车辆在其预先确定的路线上沿着路线运动通过不同的静态的路段中心的管辖区域,需要每个所述临时管辖的路段中心告知合适的密钥用于与轨道车辆进行通讯。因此,到路段中心上的密钥分配是有效的列车安全系统的基本问题,从而以运营安全的形式确保轨道车辆与所有路段中心、必要时也与其他路段运营商的路段中心进行通讯。

[0004] 图1以示意图示出了轨道车辆引导系统10的原则性构造。轨道车辆4、例如具有可控的在底部具有EVC的机动车的列车沿着路线5运动通过不同的域A、B和C,所述域处于不同的路段运营商的控制之下,并且通过点线在视觉上相互隔开。所述域A、B和C例如能够是具有各自轨道网络的国家如德国、奥地利和意大利,并且列车4例如能够具有从慕尼黑到威尼斯的计划路线5,该路线引导列车通过所有三个国家,即德国、奥地利和意大利。

[0005] 每个路段运营商具有密钥管理中心或者加密管理中心1a、1b或者1c,也称作KMC(“Key Management Centre”)。也就是说,在域A中KMC 1a对密钥管理负责,在域B中KMC 1b对密钥管理负责并且在域C中KMC 1c对密钥管理负责。在KMC 1a、1b和1c的领导下分别存在路段中心3,即所谓的RBC,密钥信息码即所谓的KMACs(“Key Message Authentication Codes”)能够由KMC获得。在此,KMACs能够包括通讯密钥,该通讯密钥能够用于使RBC 3与列车4进行可靠的通讯。

[0006] 所述路段中心或者RBC 3局部静态地对轨道网络系统的特定的闭塞段负责。RBC 3在此能够分别配属于密钥组2a、2b、2c,由各个域A、B或C中相应上级的KMC 1a、1b、1c向所述密钥组提供通讯密钥。在此能够提出,多个RBC 3配属于相同的密钥组。示例性地在域A中并且在域C中分别分配密钥组2a或者2c的两个RBC 3。也能够替代地使RBC 3同时也形成了其自己的密钥组,例如在域B中以密钥组2b示出。每个密钥组2a、2b、2c从上级的KMC 1a、1b、1c中分配地获得组所特有的通讯密钥。

[0007] 所述轨道车辆4在此通过通讯连接5a与第一域A中的RBC 3进行通讯,通过通讯连接5b与第二域B中的RBC 3进行通讯并且通过通讯连接5c与第三域A中的RBC 3进行通讯。在此,通讯连接5a、5b和5c分别通过由KMC 1a、1b、1c提供的铜须密钥保证安全。

[0008] 用于将通讯密钥分配到不同的路段中心3上的方案在于，通过列车运营员或者额相应的路段运营商的工作人员手动地分配通讯密钥。在这种情况下，工作人间能够在开始行驶之前向每个KMC 1a、1b、1c要求通讯密钥并且将该域所特有的通讯密钥安装在控制计算机上，即列车4的所谓的OBU(“On-Board Unit”)上。该安装例如能够通过经由输入接口的手动输入例如键盘或触摸屏、经由局部网络连接、局部使用的存储介质例如磁盘或USB接口的设备或安全的无线远程维护连接实现。

[0009] 这种密钥分配是麻烦的、容易出错的并且没有效率的。由此为此在不同的域的KMC之间需要持续的连接，从而确保在KMC之间持续的交换通讯密钥。

[0010] 因此，需要对于密钥分配的更简单的解决方案用于在轨道车辆的覆盖域的安全系统中的通讯密钥。

发明内容

[0011] 本发明的构思是，根据计划的列车路线制定密钥分配计划并且为了该路线的行驶自动配置了需要的通讯密钥。为此，能够通过中央负责的加密管理中心生成通讯密钥，所述加密管理中心与计划的路线进行协调。所述通讯密钥能够被提供给其他域或者路段运营商的所参与的加密管理中心，从而能够将中央的并且自动建立的通讯密钥有针对性地分配到列车以及路段中心。

[0012] 这种做法的优点是，显著简化了密钥分配计划的定义。此外，能够以简单的方式在地点和时间上限制行驶路段和行驶时间方面通讯密钥的有效性，使得按本发明的密钥分配计划比常规的密钥分配计划更不容易出错。

[0013] 另一优点是，通过自动地从外部提供的行驶路线计划生成并且证实所述计划的方案来实现密钥分配计划的可自动性。

[0014] 因此，本发明的实施方式在于一种用于分配用于对轨道车辆安全系统的交通引导信息进行加密的通讯密钥的方法，其具有以下步骤，根据轨道车辆的所计划的行驶路线在第一路段运营商的第一加密管理中心中生成通讯密钥，将通讯密钥提供给第二路段运营商的第二加密管理中心，通过第一加密管理中心将通讯密钥提供给轨道车辆以及用通讯密钥对轨道车辆的交通引导信息进行加密，从而使得轨道车辆防止被操纵地与第一路段运营商的路段中心以及第二路段运营商的路段中心进行通讯。

[0015] 有利的是，通过第一路段运营商将通讯密钥提供给第一路段中心并且通过第二路段运营商将通讯密钥提供给第二路段中心。

[0016] 根据优选的实施方式，所述通讯密钥包括多个路段中心所特有的通讯密钥，其中将所述通讯密钥提供给第二加密管理中心的步骤包括，将一组路段中心所特有的配属于第二路段运营商的第二路段中心的通讯密钥提供给第二加密管理中心。这具有以下优点，即不同的路段中心使用不同的通讯密钥，从而在不小心泄密公布的情况下或者在通讯密钥被操纵时将整个系统的丧失保持限制在仅一个路段中心上。

[0017] 根据一种实施方式，在第一加密管理中心中生成通讯密钥实现了通过密钥求导方法从主通讯密钥中导出路段中心所特有的通讯密钥。这提供了以下优点，即能够从轨道车辆本身的控制计算机中导出路段中心所特有的通讯密钥。

[0018] 根据一种优选的实施方式，通过仅用于第一路段中心的第一加密管理中心导出路

段中心所特有的通讯密钥并且通过仅用于第二路段中心的第二加密管理中心导出路段中心所特有的通讯密钥。由此能够有利地在车流量(Fahrzeugaufkommen)较高时将加密管理中心中的密钥管理仅仅限制在实际上在该加密管理中心中所需的导出的通讯密钥上。由此,在通过第一加密管理中心将通讯密钥提供给其他加密管理中心时限制数据流量。

[0019] 根据一种有利的实施方式,所述通讯密钥包括多个轨道车辆所特有的通讯密钥,其中将通讯密钥提供给轨道车辆的步骤包括,从多个轨道车辆所特有的通讯密钥中提供专门用于轨道车辆的通讯密钥。这提供了以下优点,即例如在不同的轨道车辆运营商的两个轨道车辆连接时,当相遇的轨道车辆相互调整其车辆所特有的通讯密钥时实现连接的轨道车辆相互间可靠的轨道车辆通讯。

[0020] 能够有利的是,由用于调度控制的引导系统提供轨道车辆的所计划的行驶路线,使得第一加密管理中心自动地实施通讯密钥的生成和提供。由此,一方面显著加速通讯密钥的生成和分配,另一方面能够自动校验是否沿着所计划的行驶路线生成并且分配了所有需要的通讯密钥。如此能够提早并且可靠地识别偏差和误输入。

[0021] 根据另一种实施方式,本发明实现了在第一轨道网络段运营商的第一加密管理中心中的控制装置用于分配用于对轨道车辆安全系统的交通引导信息进行加密的通讯密钥,其具有生成装置和提供装置,所述生成装置构造用于根据轨道车辆的所计划的行驶路线生成通讯密钥,提供装置构造用于将所生成的通讯密钥提供给第二路段运营商的第二加密管理中心以及轨道车辆,其中通讯密钥用于对轨道车辆的交通引导信息进行加密,使得轨道车辆与第一路段运营商的路段中心以及第二路段运营商的路段中心防止被操纵地(manipulationssicher)通讯。

[0022] 根据另一种实施方式,本发明实现了具有按本发明的控制装置、第一加密管理中心、多个第一路段中心、第二加密管理中心以及多个第二路段中心的轨道车辆安全系统,在所述第一加密管理中心中布置了控制装置,所述第一路段中心设置用于从第一加密管理中心提供由控制装置生成的用于对轨道车辆的交通引导信息进行加密的通讯密钥,所述第二路段中心设置用于从第二加密管理中心提供由控制装置生成的用于对轨道车辆的交通引导信息进行加密的通讯密钥。

[0023] 其他修改方案和变型方案由从属权利要求的特征中获得。

附图说明

[0024] 现在参照附图更精确地描述本发明的不同的实施方式和设计方案,其中:

[0025] 图1示出轨道车辆引导系统的结构的示意图;

[0026] 图2示出按本发明一种实施方式的轨道车辆安全系统的示意图;

[0027] 图3示出按本发明另一种实施方式的轨道车辆安全系统的示意图;

[0028] 图4示出按本发明另一种实施方式的轨道车辆安全系统的示意图;

[0029] 图5示出按本发明另一种实施方式的轨道车辆安全系统的示意图;并且

[0030] 图6示出用于分配通讯密钥的方法的示意图,所述通讯密钥用于对按本发明另一种实施方式的轨道车辆安全系统的交通引导消息进行加密。

[0031] 只要有意义,所描述的设计方案和改进方案就能够相互任意组合。本发明的其他可能的设计方案、改进方案以及执行方案也包括本发明的前面或者后面关于实施例所描述

的特征的没有详尽提到的组合。

[0032] 附图应该促成对本发明实施方式的进一步理解。附图说明了实施方式并且与说明书共同用于解释本发明的原理和构思。其他实施方式以及多个所述的优点参照附图获得。附图的元素不必要相互按照比例示出。在此，相同的附图标记表示相同或者类似作用的组件。

具体实施方式

[0033] 在下面说明的意义上，通讯密钥包括所有加密信息和数据单元，其适合于对明文格式的数据进行加密并且由此生成防窃听和/或防读取的密文格式的数据，或者其适合于保护明文格式的数据的完整性并且实现加密的校验和(Prüfsumme)，并且其还适合于在加密信息的识别中由密文格式的数据恢复明文格式的数据或者校验所述数据在传输期间没有被处理过。本发明意义上的通讯密钥例如能够包含对称的密钥对、非对称的密钥对或者类似的加密方法。在此例如能够通过例如AES、DES、KDF、IPsec、SSL/TLS、MACsec、L2TP、PPTP、PGP、S/MIME这样的方法使用通讯密钥或者通过所配属的密钥管理例如IKE、EAP或其他方法使用类似的技术。

[0034] 图2示出了轨道车辆安全系统20的示意图。该轨道车辆安全系统20与图1中所示的轨道车辆引导系统10的区别在于，在所述加密管理中心(Schlüsselvergabestelle)1a、1b、1c(KMC)中的每个中都布置有控制装置7，所述控制装置设置用于生成和分配用来对交通引导消息进行加密的通讯密钥。在此，所述控制装置7例如能够是软件模块，所述软件模块在所述KMC上起作用并且构造在所述KMC上。

[0035] 所述控装置装置7包括用于生成用于加密保护轨道车辆4的交通引导消息的通讯密钥6的生成装置。在下面的实施例中假设，所述轨道车辆4配属于域(Domäne)A，从而使得所述KMC 1a是轨道车辆4的所谓的“根KMC(Heim-KMC)”，也就是说在控制KMC 1a的情况下进行通讯密钥的生成和分配。其余的KMC 1b和1c在这种情况下取决于通过KMC 1a进行的控制。当然在其他情况下、例如用于其他轨道车辆时，同样能够使其他KMC 1b和1c承担根KMC的角色。在此，KMC 1b和1c的控制装置7与KMC 1a的控制装置7构造得一样。此外，KMC 1a、1b和1c的数量当然也不限制于三这个示出的数量。同样能够有其他任意数量的KMC。在此，KMC 1a、1b、1c尤其能够由不同的路段运营商(Streckenbetreiber)运营。

[0036] 所述生成装置能够设计用于在步骤8a中根据轨道车辆4的计划的行驶线路生成通讯密钥6。在此，所述生成装置能够设计用于，由(未示出的)调度控制系统或行程答询系统自动地提供所计划的行驶路线。

[0037] 通讯密钥6能够通过第一KMC 1a随后在步骤8b中提供给第二KMC 1b并且在步骤8c中提供给第三KMC 1c。被提供通讯密钥6的KMC 1b、1c在此根据轨道车辆4的计划的行驶路线进行调整。KMC 1b、1c例如能够对路段中心3负责，轨道车辆4的计划的行驶路线穿过其引导区域。通讯密钥的提供在此能够通过控制装置7的提供装置来实现。

[0038] 在步骤9a中能够将所生成的通讯密钥6分配到第一域A的第一路段中心3(RBC)上。此外，能够在步骤9a中将通讯密钥6安装在轨道车辆4的控制计算机(EVC)上。所述通讯密钥6能够在步骤9b和9c中通过KMC 1b和1c提供给域B或者域C中的RBC3。

[0039] 所述KMC 1a能够在实现通讯密钥6的分配之后进行操纵，使得轨道车辆4能够投入

使用并且能够驶过域A、B和C。当例如由于路段封锁或者轨道车辆4的其他改道而应该驶过其他(未示出的)域D,对于所述域而言没有向各个路段中心3提供通讯密钥6时,能够建立修改的密钥分配计划,其中在通过操作员相应的授权之后所述控制装置7将通讯密钥6也传递到域D的KMC上,所述KMC本身将通讯密钥继续分配到其域D的RBC3上。作为替代方案能够向操作员显示,所述轨道车辆4仅仅有资格通过域A、B和C,但是没有资格通过其他域。

[0040] 图3示出了轨道车辆安全系统30的示意图。所述轨道车辆安全系统30与图2中的轨道车辆安全系统20之间的区别在于,该通讯密钥6包括多个专门为域或者专门为路段中心生成的通讯密钥6a、6b、6c。在此,所述通讯密钥6a、6b、6c中的每个通讯密钥都为RBC3区域特定地生成。在此,通讯密钥6a、6b、6c能够随机地或者伪随机地或者借助于密钥求导函数从基本密钥和/或取决于RBC的求导参数中生成。所述通讯密钥6a、6b、6c共同地安装在轨道车辆4的控制计算机上。

[0041] 随后从通讯密钥6a、6b、6c中选出通讯密钥组,所述组能够配属于相应的域B和C的相应的RBC 3。随后在步骤8b、8c中仅仅传输需要KMC 1b、1c来提供给其RBC的通讯密钥6b和6c。

[0042] 所述轨道车辆4能够在穿过域A、B和C时根据当前的位置选出通讯密钥6a、6b、6c中相应的一个,从而与相应的域的瞬时当前的RBC3进行通讯。当前位置例如能够经由卫星导航系统、例如GPS或GALILEO通过无线电基站的定向、例如经由GSM-R或者WLAN借助轨道网的路段计算机的地址或者识别码或者通过欧洲应答器例如铁路路基上的固定数据应答器或者透明数据应答器求得。

[0043] 图4示出了轨道车辆安全系统40的示意图。该轨道车辆安全系统40与图3中的轨道车辆安全系统30的区别在于,在KMC 1a、1b和1c之间设置了主通讯密钥6,从中能够通过密钥求导函数导出多个通讯密钥6a、6b、6c。在步骤8b和8c中代替多个通讯密钥6a、6b、6c将主通讯密钥6传递到KMC 1b和1c上,所述KMC本身能够局部地导出多个通讯密钥6a、6b、6c。通过KMC的求导例如能够根据列车所特有的参数、例如轨道车辆4的识别码实现。所述主通讯密钥6在此例如能够仅仅在特定的时间段上有效。

[0044] 同样能够规定,所述轨道车辆4本身以主通讯密钥6来提供,轨道车辆4的控制计算机从中导出多个通讯密钥6a、6b、6c本身。

[0045] 例如能够借助于密钥求导函数(Key Derivation Function,KDF)例如HMAC(哈希信息验证码)或者AES-CBCMAC(高级加密标准-加密字组链接信息验证码)根据RBC所特有的参数例如识别码、区域码、路段码或类似参数从主通讯密钥6中导出多个通讯密钥6a、6b、6c。

[0046] 这种做法的优点在于,不必在KMC 1a、1b、1c之间形成持续的在线连接,因为每个KMC能够自动地从传递一次的主通讯密钥6中导出RBC所特有的通讯密钥6a、6b、6c,而为此不需要重新与根KMC 1a进行通讯。此外,在多个轨道车辆4和RBC 3中只需要在KMC 1a、1b、1c之间交换少量的数据。

[0047] 图5示出了轨道车辆安全系统50的示意图。该轨道车辆安全系统50与图4中的轨道车辆安全系统40的区别在于,设置了主通讯密钥6,从所述主通讯密钥中能够经由密钥求导函数导出多个轨道车辆所特有的通讯密钥6a、6b、6c。从例如在图5中配属于轨道车辆4的轨道车辆所特有的通讯密钥6c中能够再次导出多个RBC所特有的通过各个KMC 1a、1b、1c能够

分配到不同的RBC 3上的通讯密钥11。为轨道车辆4提供了各个轨道车辆所特有的通讯密钥6c以及RBC所特有的通讯密钥11，从而能够通过选出RBC所特有的通讯密钥11之一来实现与相应RBC 3的通讯。

[0048] 例如能够规定，在两个轨道车辆上为不同的运营商或者不同的根KMC安装相同的轨道车辆所特有的通讯密钥6c，从而在两个轨道车辆耦合时实现可靠的轨道车辆通讯。

[0049] 图6示出了用于分配用来对轨道车辆安全系统的交通引导信息进行加密的通讯密钥的方法60的示意图。在第一步骤61中，根据轨道车辆的计划的行驶路线在第一路段运营商的第一加密管理中心(KMC)中生成通讯密钥。在第二步骤62中，将通讯密钥提供给第二路段运营商的第二KMC。在第三步骤63中，通过第一KMC将通讯密钥提供给轨道车辆。在第四步骤64中，用通讯密钥对轨道车辆的交通引导信息进行加密，使得轨道车辆防止被操纵地与第一路段运营商的RBC以及第二路段运营商的RBC进行通讯。对交通引导信息进行加密尤其理解为，加密保护使用数据和/或管理数据、例如寻址信息、交通引导信息不被窃听和/或操纵，例如通过相应加密的加密数据代替明文数据，和/或通过添加加密的完整性校验信息(信息验证码)。

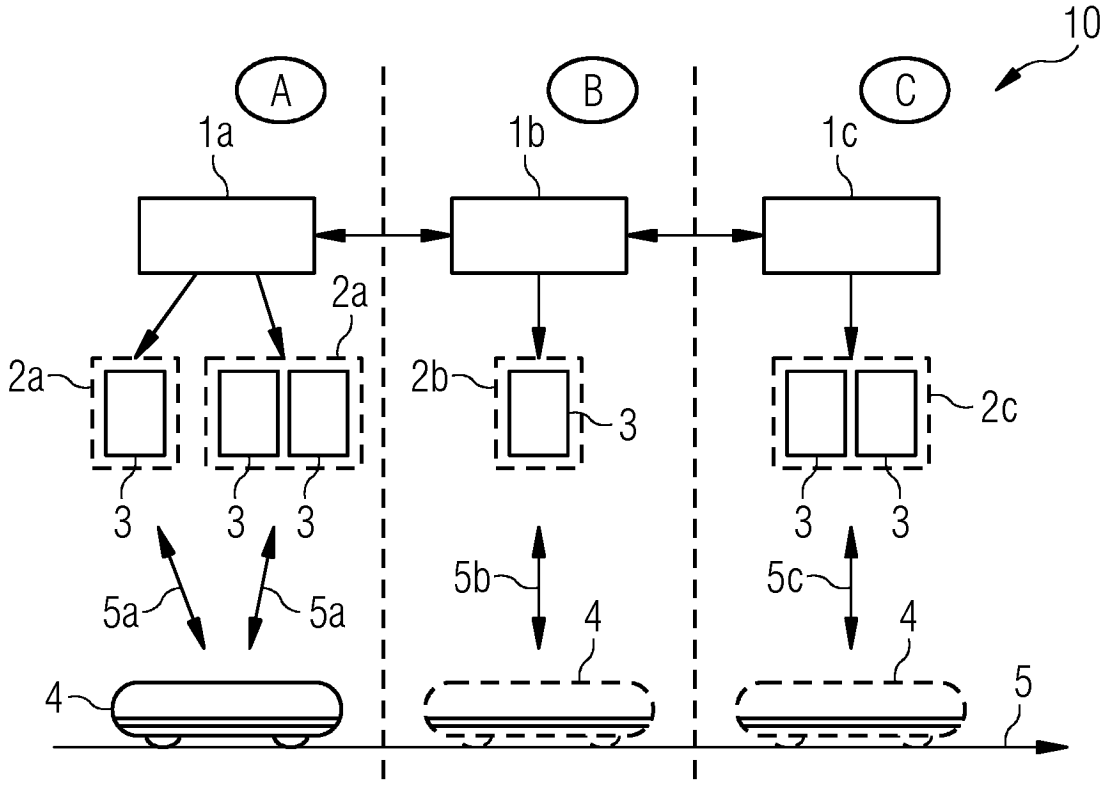

10
A
B
C
1a
1b
1c
2a
2a
2b
2c
3
3
3
3
3
3
3
5a
5a
5b
5c
4
4
4
4
5

图 1

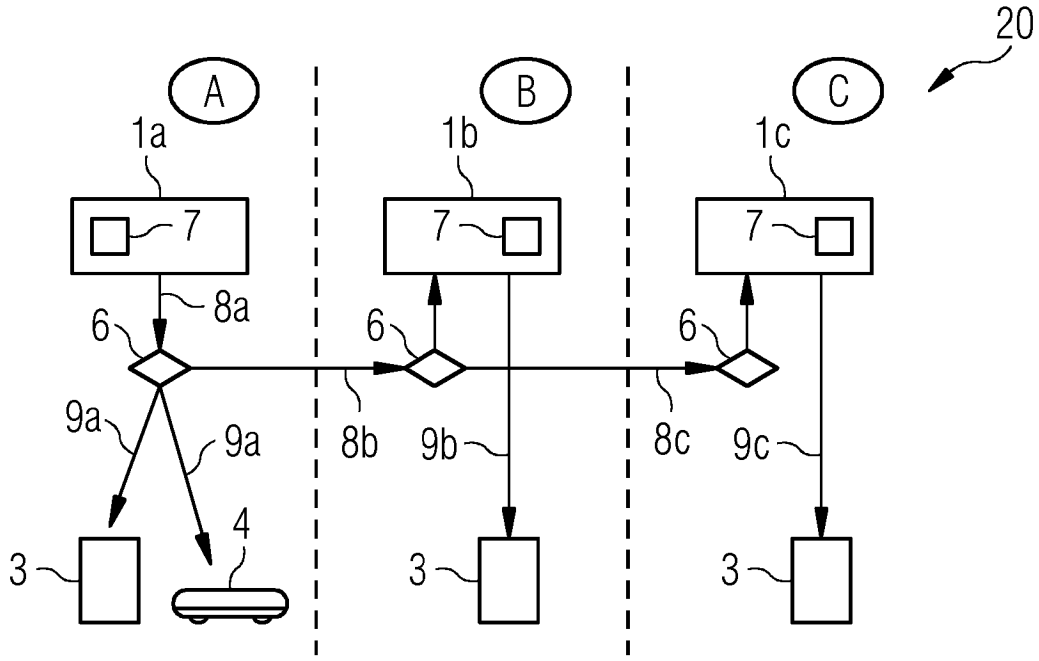

20
A
B
C
1a
1b
1c
7
7
7
6
6
6
8a
8b
8c
9a
9a
9b
9c
4
3
3
3

图 2

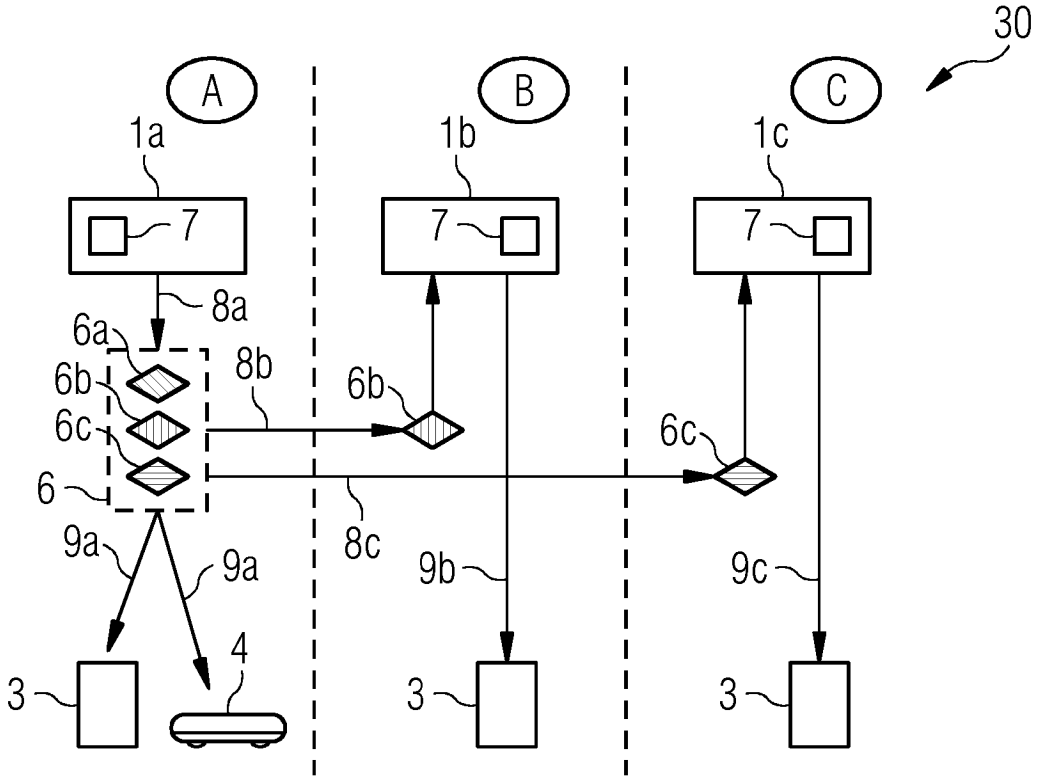


图 3

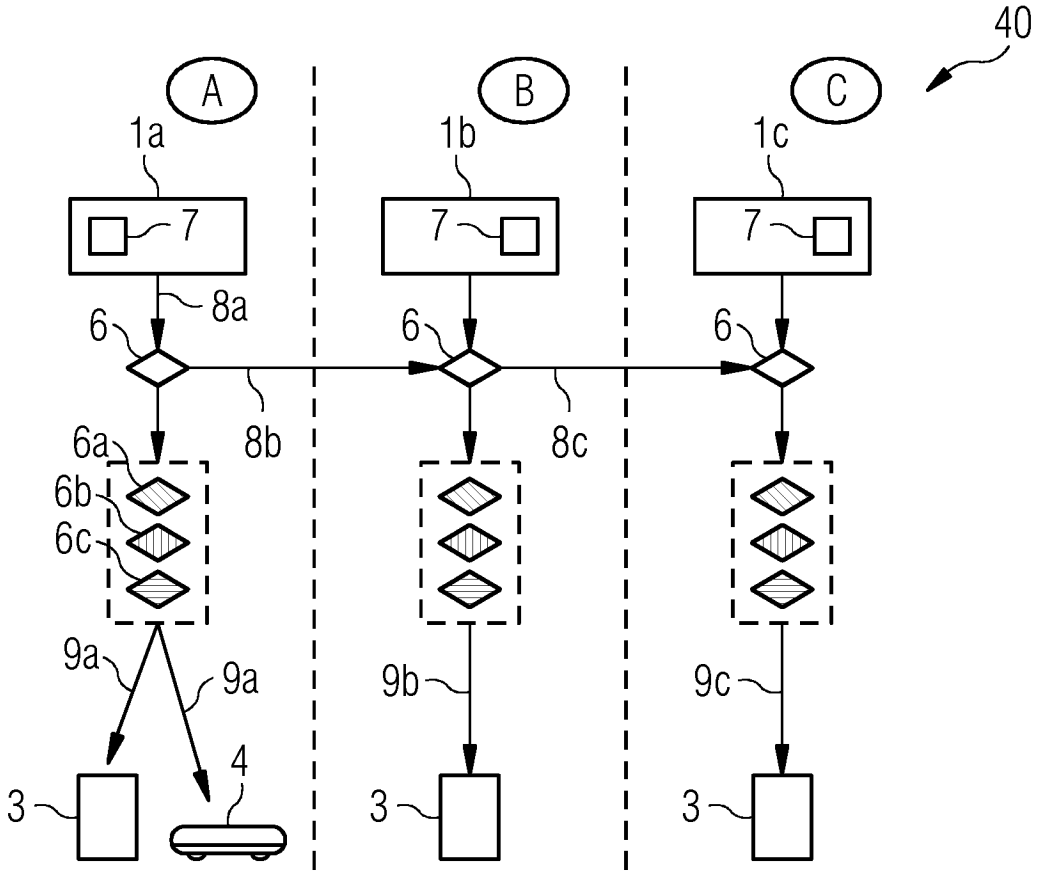


图 4

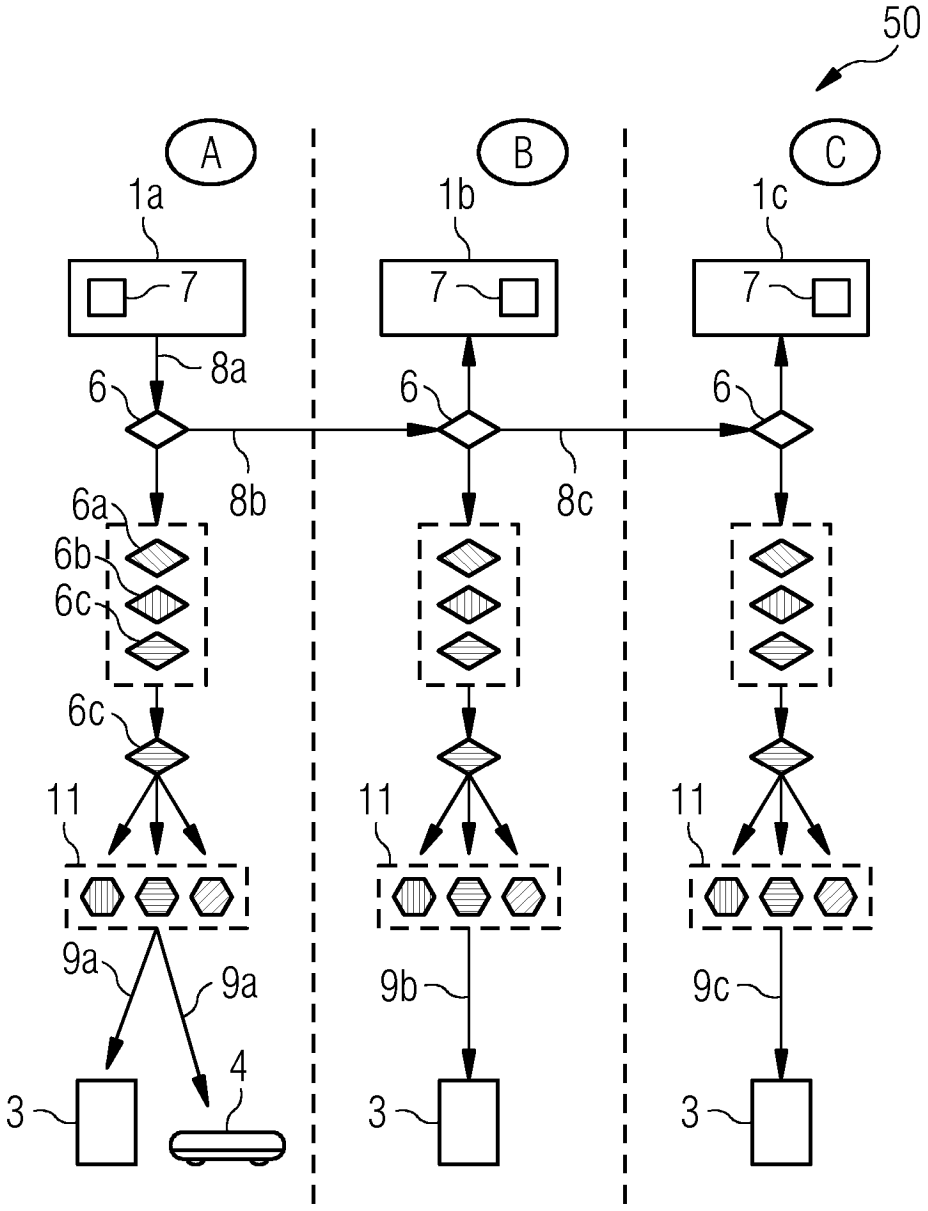


图 5

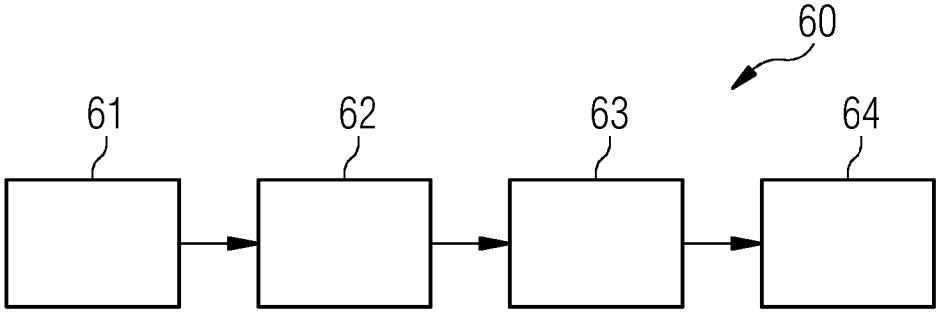


图 6