

(12) 发明专利申请

(10) 申请公布号 CN 102216735 A

(43) 申请公布日 2011.10.12

(21) 申请号 200980146356.3

(71) 申请人 IAD 信息自动化及数据处理有限公司
地址 德国大哈伯斯多夫

(22) 申请日 2009.11.18

(72) 发明人 H·汉佩尔 G·布米勒

(30) 优先权数据

102008058264.6 2008.11.19 DE

(74) 专利代理机构 中国国际贸易促进委员会专利商标事务所 11038

(85) PCT申请进入国家阶段日

2011.05.19

代理人 赵科

(86) PCT申请的申请数据

PCT/EP2009/008225 2009.11.18

(51) Int. Cl.

G01D 4/00 (2006.01)

(87) PCT申请的公布数据

W02010/057631 DE 2010.05.27

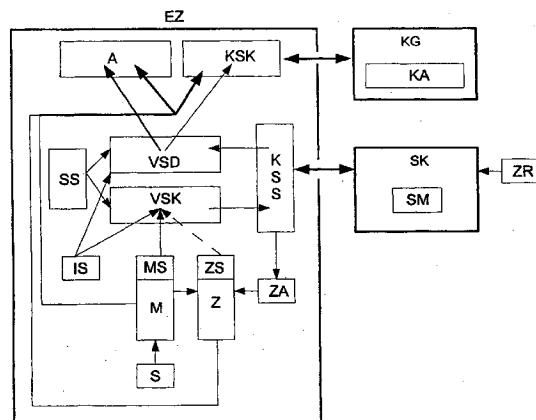
权利要求书 2 页 说明书 14 页 附图 5 页

(54) 发明名称

计量装置、尤其是计能表以及识别篡改的方法

(57) 摘要

已知不同型式的抄表系统,其当今通常统称为AMM系统(AMM:自动计量管理)。但实践中缺少不仅能独立于其它现有技术条件普遍应用且能使用户现场自行监控(用量/泄漏等)的用量表和篡改识别方法。按照本发明,能将系统通过数据通信返回的计量数据识别为自己的数据且杜绝篡改计量值、并从而可靠地提供这些返回的计量数据供继续处理/公析或者显示(A)的与至少一个系统进行数据通信的计量装置(EZ)主要包括:至少一个加密和/或签名编码器(VSK),该编码器利用密钥存储器(SS)中的密钥将用来检查数据完整性的信息配备给提供给上述存储器(IS、MS和ZS)的包括有效和可信标记的信息,在一当前数据集中进行组合,且至少交给通信接口(KSS)进行传输,仅有一部分先前的数据集或其内容保存在计量装置(EZ)中;至少一个加密和/或签名解码器(VSD),该解码器可利用密钥存储器(SS)中的密钥检查通过通信接口(KSS)返回的具有计量值的数据集以确定数据内容的完整性及计量装置(EZ)的标识符,并在检查结果为肯定的情况下提供这些数据供继续处理/分析或者显示(A)。本发明涉及用于综合采集用量数据的计量装置以及系统。



1. 一种与至少一个系统进行数据通信的计量装置 (EZ), 能够将该系统通过数据通信返回的计量数据识别为自己的数据并且能杜绝对计量值的篡改, 从而能可靠地提供返回的这些计量数据供进一步处理 / 分析或者显示 (A), 所述计量装置具有:

- 用于与至少能够接收经过签名和 / 或加密的计量值、能够将这些经过签名和 / 或加密的计量值保存在存储器 (SM) 中、并且能够返回这些经过签名和 / 或加密的计量值、而且能够提供相对于时间基准 (ZR) 的时间信息的系统的组件 (SK) 连接的至少一个通信接口 (KSS),

- 至少一个计量模块 (M), 该计量模块将至少一个传感器 (S) 提供的计量信号对应于能量计量值或者计量表读数,

- 至少一个用于保存上次确定的能量计量值或者计量表读数 (简称为计量值) 的存储器 (MS),

- 至少一个时间戳存储器 (ZS), 用于保存针对上次产生的计量值在时间模块 (Z) 中确定的时间戳,

- 至少一个时间调整模块 (ZA), 该时间调整模块检查系统通过通信接口 (KSS) 提供的时间 (ZR), 并且跟踪时间模块 (Z) 中的本地时间,

- 至少一个用于保存分配给计量装置 (EZ) 的标识符的存储器 (IS),

- 至少一个用于保存加密和 / 或签名所需的密钥的存储器 (SS),

- 至少一个加密和 / 或签名编码器 (VSK), 该编码器通过使用密钥存储器 (SS) 中的密钥为提供给上述存储器 (IS、MS 和 ZS) 的包括有效标记和可信标记的信息配备以用于检查数据完整性的信息, 组合成当前的数据集并且至少提供给通信接口 (KSS) 进行传输, 其中以前的数据集或者其内容仅有一部分被保存在计量装置 (EZ) 中, 以及

- 至少一个加密和 / 或签名解码器 (VSD), 该解码器能通过使用密钥存储器 (SS) 中的密钥对通过通信接口 (KSS) 返回的具有计量值的数据集进行检查以确定数据内容的完整性以及计量装置 (EZ) 的标识符, 并且在检查结果为肯定的情况下提供这些数据供进一步处理 / 分析或者显示 (A)。

2. 根据权利要求 1 所述的计量装置, 其特征在于, 所述计量装置具有用户接口 (KSK), 并且通过所述用户接口将已经检查过数据内容的完整性和标识符的数据集传输给用户的任意的合适的设备 (KG), 该设备具有自身的显示器 (KA) 或用于转发给具有显示器的设备。

3. 根据权利要求 1 所述的计量装置, 其特征在于, 序列号或者系统运营者的资产编号被保存在标识符存储器 (IS) 中。

4. 根据权利要求 1 所述的计量装置, 其特征在于, 时间模块 (Z) 控制本地时间和日期。

5. 根据权利要求 1 所述的计量装置, 其特征在于, 使用世界协调时 UTC、尤其是 (德国) 联邦物理技术研究所的 UTC(PTB) 作为时间基准 (ZR)。

6. 一种用于对经过认证和 / 或检定的计量装置 (EZ) 的篡改进行识别的方法, 在所述方法中:

- 生成至少包含标识符 (IS)、时间值 (ZS)、计量值 (MS) 和签名 (SS) 的数据包,

- 所述数据包被传输给未经认证和 / 或检定的系统或者该系统的组件 (SK), 所述系统或者该系统的组件保存这些数据包或者相关部分 (SM), 并且根据计量装置的请求将这些数据包或者相关部分返回给计量装置 (EZ),

- 在此期间,这些数据包或者其内容不被保存在计量装置 (EZ) 中,
- 计量装置 (EZ) 能以安全性得到证实的方式借助于密钥 (SS) 和签名,对由所述系统或者由所述系统的组件 (SK) 提供的数据包或者其相关内容进行验证以确定数据包的数据是否未被更改以及是否来自于该计量装置 (EZ),
 - 在经过检定认证的显示器 (A) 上以与没有离开计量装置 (EZ) 的计量值相同的可信状态显示经过成功验证的数据。

7. 根据权利要求 6 所述的方法,其特征在于,经过成功验证的数据被提供到计量装置 (EZ) 的接口 (KSK) 供进一步处理 / 分析或者显示 (A)。

8. 根据权利要求 6 所述的方法,其特征在于,使用网络时间协议 NTP 来通过公共网络将系统的时间基准 (ZR) 传输给计量装置 (EZ)。

9. 根据权利要求 6 所述的方法,特征在于,所述方法用于计能表 (EZ)。

10. 根据权利要求 6 所述的方法,其特征在于,用户控制地通过计量装置 (EZ) 的用户接口 (KSK) 和 / 或通过计量装置 (EZ) 上的按钮或者通过通信 / 控制模块 (COM) 或者通过 MUC (公用事业通信系统) 查询计量值。

计量装置、尤其是计能表以及识别篡改的方法

技术领域

[0001] 本发明涉及权利要求 1 所述的一种计量装置,尤其是用于可靠采集并且显示读数数据的计能表,本发明还涉及权利要求 6 所述的一种用于识别篡改的方法。

背景技术

[0002] 当今可在不同的物理计量点采集不同类型家用能源的用量数据(电流,冷水,热水,热量,冷量,燃气,燃油或者类似物质)。这些统称为多应用(MultiUtility)的公用事业均有以下特征:

- [0003] ➤需要不怀疑发票中的计量值和检定值(关键字:保护消费者),
- [0004] ➤将本地以数字形式显示的计量值传输给控制中心以及这里的处理系统,
- [0005] ➤迅速按时间和用量开具发票,通过现金管理系统进行监控,以及
- [0006] ➤需要为所有供应类型提供一种统一的解决方案。

[0007] 迄今为止计量装置的技术发展以及用于综合采集用量数据的系统均具有一些典型的弱点和问题,如缺乏统一性,或者仅适合于某些方面的个别解决方案。诸如供能或供水公司之类的公用事业公司通常均根据用户的用量表读数数据开具资费账单,这些用量表多数均安装在使用点附近。用量表可以是例如燃气表、水表、电表、热量表、供暖分户计量表等等,之前消费期的计量表读数数据是反映使用点的用量的尺度。通常至少每年一次采集某一房屋、住所或个别使用点的计量表读数数据或计量表读数。

[0008] US 6,538,577B1 公开了一种以两种不同方式在用量表与公用事业公司(用量数据采集中心)之间进行通信的电子计量表(用量表)。可采用间接方法与用量数据采集中心进行通信,即利用双向无线传输装置(双向无线收发器)通过无线 LAN(900MHz 局域网络,双向,扩频)连接到一个网关节点(网关),该网关通过一个市面上可以买到的双向固定 WAN(广域网络)与用量数据采集中心相连。若采用直接方法,则将一个网络接口(PLC 模块→通信网络模块)插装在计量表电路板的背面上。这时要跳过 LAN 或网关(旁路,因为这里不需要使用)。用量表采用模块化设计,可移去、更换计量表内的电路板和模块,这些电路板和模块均插装在同一个背板上,可用于传输用量数据和电力质量。网关布置在远离计量表之处,并且具有四个组件,即 WAN 接口模块、初始化 μ C、扩频处理器和射频收发器。无线收发器也可以接收无线收发器所包含的其它计量表的用量数据,并且可将其转发给用量数据采集中心。按照 US 6,538,577B1 所述,仅在(LAN) 无线模式下在用量表和网关之间交换数据。

[0009] 此外在专利申请书 EP 1 677 270 A1 中还描述了一种用于构建 AMR 网络(自动抄表)的方法,包括以下组件:

- [0010] • 计量表,
- [0011] • 收集单元(Gathering Units)(例如电表或者终端单元),
- [0012] • 集中器(通常;工业计算机),
- [0013] 并且有三种连接类型:

[0014] • LPRB(低功率射频或蓝牙),

[0015] • PLC(电力线通信),

[0016] • MC(移动连接,尤其通过移动电话),

[0017] 可用于在AMR网络中建立最佳连接。在至少一个收集单元中在LPRB(输入端)和PLC(输出端)进行转换。

[0018] 此外WO 2008/086231A2还公开了一种移动式用量数据采集系统和一种用于无线抄读用量表以及重新配置AMR用量数据采集系统的方法。用量表可以是例如利用无线接口合并在一个终点站中的燃气表、水表、电表、热量表、供暖分户计量表等等。抄表人员可使用无线数据接收装置完成数据采集,将无线数据接收装置依次置于将要以无线方式抄读的用量表的发射范围之中即可。采用车载抄表装置(drive-by unit),利用一辆汽车使得移动式无线数据接收装置沿着街道移动,街道旁的房屋均安装有用来采集用量数据的“无线”用量表。移动式无线收发器可用来将相关用量表利用无线接收装置接收的计量表读数数据与计量表识别数据一起发送给集中数据采集点。通过移动无线系统(单向或双向无线连接)在移动的时间间隔之内将所发送的数据传输给集中数据采集点,所述时间间隔从计量表数据输入到数据接收装置之中时开始。此外还可以利用例如GPS无线定位系统采集用量表的位置信息,并且通过移动无线系统将其从数据采集点发送给数据采集人员的移动无线终端设备。如果某一个计量表被意外忽略,或者由于某个缺陷、故障以及类似情况而没有发送信号,或者无法正确将其复位,就会将这种情况自动记录在集中数据采集点之中,因为从该计量表没有包含识别数据的预期数据集到达集中数据采集点。利用CRC码验证接收数据的完整性或有效性,计量装置利用“收据”消息形式的“应答”描述正确数据接收的验证。然后集中数据采集点就可以自动通过移动无线系统将未采集的用量表的信息反馈给抄表人员。抄表人员可以将组合装置重新置于用量表的额定无线作业范围之内,以便查找更有利于接收的位置,接收相关用量表的数据报文(计量表读数数据、计量表识别数据、位置信息数据)。

[0019] 为了不仅能够实现集中数据采集和远程抄表,也就是以经济方式协调所有用量的抄读服务,而且也为了能够根据计量值/历史记录进行能源控制,欧洲专利申请书EP1 850 500 A1公开了一种数据采集和控制系统,包括:

[0020] • 至少一个与天线相连的无线模块,用于连接某个设备或用量表中至少一个配有无线发射器和/或者无线接收器的远程模块,

[0021] • 一个与无线模块相连的控制装置,具有一种程序和用来临时保存无线模块所提供的数据的数据存储器,

[0022] • 一个与控制装置相连的通信模块和一个与其相连的第一耦合模块,用于通过供电线路传输所提供的数据,以及

[0023] • 一个通过通信模块和与其相连的第二耦合模块与供电线路相连的通信网关,该网关安装于总电表之处,

[0024] 使得通信网关与家中的供电线路一起形成用于传输数据的骨干网络,并且在组合无线/电力线模式下利用通信网关在远程模块或用量表之间交换数据。

[0025] 欧洲专利申请书EP 1 850 500 A1所述数据采集和控制系统中的数据传输方法的特征在于:

[0026] • 无线模块用来连接远程模块或用量表,

- [0027] • 通信网关承担节点作用，并且与集中计量点或传输点之间传输数据，
[0028] • 通信网关与家中的供电线路一起形成用于传输数据的骨干网络，
[0029] • 利用通信网关在组合无线 / 电力线模式下在远程模块或用量表之间交换数据，并且
[0030] • 通信网关构成公用事业、安全技术、住宅和楼宇管理、自动化技术领域其它增值服务的接口以及家庭自动化包括能源控制领域的服务接口。

[0031] 多年以来通常使用的电表均具有两个或更多能够结算不同费率的计数机构，可通过内置或者外接的脉动控制接收器（通过供能公司的中央脉动控制设备对其进行控制）或者通过费率转换定时开关在这些计数机构之间进行转换。几年以来新开发的计能表均不含机械元件。例如可通过具有软磁环形铁心的电流互感器（或者具有罗戈夫斯基线圈的电流测量系统）利用并联电阻或者霍尔元件来检测电流。利用电子电路计算电能，然后将结果提供给字母数字显示器（多数是液晶显示屏，LCD）。对于特殊合同用户（工业）通常也可将其它计数机构用于计量功率。但在实践中正逐渐转为采用具有负荷曲线记录供能的电子计量表。这样无需干预计量表就能改变费率，并且在计量表中不再需要独立的计数机构。

[0032] 供能公司和楼宇自动化系统可以通过数据接口以远程查询方式对某些电子计量表进行抄读。实践中通常使用红外、S0 接口、M 总线、与 GSM、PSTN 调制解调器或者 PLC 模块相连的干接点作为数据接口。目前在联邦德国（从 2006 年 4 月起）也将利用互联网连接 (DSL) 进行现场试验。在美国已经开发出内置有一个继电器的电子家庭计量表，除了能实现远程抄读之外，还使得供电公司能够实现遥控切断，例如当账单欠费时。德国正在智能计量技术推广示范项目范畴内逐渐使用智能计量表。脉冲输出端 (S0) 通常可提供每千瓦时包括 2000 ~ 5000 个脉冲的用量数据信号。然后必须根据计量表将该值乘以一个固定系数，例如 30 或 50，以便获得累计的计量值。

[0033] 此外还有众所周知的投币式计量表，或者可通过芯片卡、芯片钥匙或者输入 PIN 码调出定量电能的预付费计量表。例如在德国就将此类计量表用于自动洗衣店，或者供能公司将其用于付款信用差的用户。

[0034] 不仅可根据所使用的能量（千瓦时），而且还可根据平均使用功率（千瓦）计算大客户的用电量。为此可安装能够每隔 15 分钟测定并且保存平均使用功率的负荷曲线计量表（1/4 小时功率计量）。通常以远程查询方式抄读这些计量表。对于较小的用户则可根据一种标准负荷曲线（例如适用于家庭用户的 H0）模仿负荷曲线。

[0035] 商用电表在联邦德国必须接受检定。在检定有效期结束之后（电子计量表为 16 年或 8 年，具有感应机构也就是具有转子圆盘的机械互感式计量表为 12 年），就必须更换计量装置或者延长检定有效期。

[0036] 从 2008 年起开始的现场试验中，总计将 2000 个时钟同步式负荷曲线计量表分配到不同的公司，这些计量表均利用短信语言 SML（智能消息语言：Smart Message Language）进行通信（交换计量数据，但也可更新固件），这是类似于工业标准可扩展标记语言 XML 的一种语言，并且同样也对其进行了测试。这将替代迄今为止制造商专用的计量表查询指令。传统的负荷曲线计量表内均安装有一个实时时钟，可在停电之后跳转到某一预先定义的启动时间。如果在两次抄表期间多次出现这种故障，由于不再存在正确的时间基准，并且不同计量表的时间大相径庭，因此就不会使用计量值。

[0037] 有不同的方法可解决这个问题。有几种负荷曲线计量表使用实时时钟和定期调整时钟的同步方法。按照时钟同步式负荷曲线计量表的规范,安装一种(秒)计数器替代实时时钟。该计数器的读数随着每一秒的逝去单调增大,可用来明确标识电表读数。抄读了时钟同步式负荷曲线计量表之后,将秒指针与绝对时间关联起来。如果该计量表出现(多次)电压中断,测量值组的顺序可保持清晰。时钟同步式负荷曲线计量表可分为一个基本单元和不同的模块,所有制造商的基本单元和模块均应当兼容。基本单元仅提供计量表的基本功能,与必须检定的单元一样。可以插装模块型式的所有其它功能,诸如与其它设备或通信单元(例如GSM或者GPRS模块)。因此不必开发或购买、储存专用于每一种应用的设备。另一方面变得越来越重要的是保证根据计量表读数数据开具资费账单,防止篡改。主要着眼点是识别篡改,尤其是用户打开通常有铅封的计量表外壳。

[0038] 例如WO 2006/048143A1就公开了能够以可靠、节能方式识别非法篡改用量表外壳的一种装置,没有机械操作的按钮或者电磁开关或光栅。具体而言,该装置包括一个容纳电子分析装置的第一壳体部分以及一个可以与第一壳体部分分开的第二壳体部分,并且锁定了第一壳体部分,可防止非法移去第二壳体部分。在第一壳体部分中采用一个由线圈和电容构成的振荡电路,在第二壳体部分中有一种金属材料,当线圈与金属材料之间的距离改变时,线圈就会产生信号,并且将该信号提供给第一壳体部分中的串联电子分析装置继续进行处理。如果振荡电路的衰减强度以及电路的脉冲响应时间下降,振荡电路的线圈性能就会变化,从而识别出从第一壳体部分上移去了第二壳体部分。适宜将本发明所述装置的振荡电路设计成耗电量很少的接近开关。能量很少的短促电压脉冲就足以激励振荡电路。如果同时以比较低的周期(例如每隔十秒钟)进行激振,则本发明所述监控电路的平均所需功率极少,因此使用一次或二次电池或者高容量电容也能在很长时间内工作。脉冲响应时间与振荡电路的衰减强度有直接关系,可利用微处理器电路对其进行分析。

[0039] WO 2004/021020A1公开了一种防止非法篡改的类似方法,在计量表的壳体中利用一个遮盖计量表接线端子的铅封壳盖将至少另一个计量装置盖住,利用第二个铅封防止对其非法篡改。另一个需要保护的计量装置的铅封经过适当设计,使其在没有接线端子盖板的状态下可以自由够着,从而便于快速对其进行检查。为此计量表壳体具有至少一个铅封扣,附加盖板的铅封孔与其共同作用,铅封钉穿过至少一个铅封扣和铅封孔起到连接件作用。特别有益的方式是将至少一个铅封扣与铅封孔相隔一定距离,从而可以看见铅封钉的预定断裂点,尤其可看见在其之间的透明铅封钉。

[0040] 电子计量表通常具有用来检测、量化显示用电量信息的电子电路,当停电或者以其它方式中断交流电源时,就会产生另一个问题。为此已经开发出能够在识别交流电源中断时将重要数据写入到非易失性存储器之中例如写入到可擦写、可编程的只读存储器(EEPROM :electrical erasable programmable readonly memory)之中的方法。有一些计量装置也包括电池,可允许数字电路部件在停电期间在减额模式下工作,从而可使得时钟和其它电路能够在停电期间继续工作。为了能够在计量表的外部交流电源中断期间进行抄表,DE 600 01358 T2公开了一种电子计量表,能够在计量表的交流电源中断期间识别操作人员激活的显示请求信号(例如按下某一个按钮开关),然后就会在有限的时间内显示计量表读数信息,作为对显示请求信号的反应。具体而言,电子计量表包括一个测量电路与一个用电量处理电路,所述用电量处理电路从传感器电路(电流互感器、电流测量电阻、线圈

或类似器件)获得模拟测量信号,并且将原始用电量数据和其它数据提供给处理器、非易失性存储器和显示装置。此外测量电路还包括给上述元器件提供偏置电流的电路,包括电源、停电识别电路、第一备用电源和第二备用电源。可在电流中断期间通过备用电源提供用于显示的电流,因此所提供的电流很小,因为仅作为对操作人员激活的显示请求信号的反应而进行显示,而且仅在有限的时间内显示计量表读数信息。在正常工作期间可以显示第一批挑选出来的计量表读数信息,在交流电中断期间则可以显示第二批挑选出来的计量表读数信息。第一批挑选出来的计量表读数信息可以与第二批挑选出来的计量表读数信息相同或者不同。用户可以对所产生的计量表读数信息的一部分进行编程,形成第一批和第二批挑选出来的需要显示的计量表读数信息。上述用来在交流电中断期间提供电子显示用量信息的装置很容易安装到其它类型的电子用量表之中,包括燃气表、水表或其它用量表。

[0041] 能源市场自由化带来的另一个问题是最终用户可以购买任意供电公司的电力。为了实现远程抄表,尤其为了能够自动处理随时间变化的不同用量,DE 10024 544 A1 公开了一种装置,其中的数据采集装置与用量表耦合在一起,可从用量表获得相应的用量数据,将这些用量数据对应于某一个绝对时间,然后据此生成传输数据,所述传输数据具有相互对应的时间数据和用量数据。连接在数据采集装置后面的是一种用来在较大距离范围内传输数据的远程传输路径(例如 ISDN 数据传输路径、互联网连接、模拟电话连接、无线传播路径以及其它适用的数据传输路径)。最终与远程传输路径相连的是一个用来接收、分析传输数据的数据处理装置,可采集所时间数据变化的用量数据。数据采集装置具有一个存储装置,该存储装置可收集、临时保存传输数据,然后将所收集的数据传输给数据采集装置。可以在一定的时刻传输所收集的数据,可以与一定的事件相互关联,或者由数据处理装置或数据采集装置发起传输所收集的数据(例如当数据采集装置中存储一定的数据量时)。除了传输数据之外,还可将用于标识和识别用量表的识别数据从数据采集装置传输给数据处理装置。在停电时无法访问数据采集装置,但是所保存的数据依然保留不变。可以记录并且随时调出停电持续时间。在停电之后,例如数据采集装置可以请求当前的日期和当前的时钟时间,并且将发生了停电的消息传输给数据处理装置。从停电开始起使用零填充计量表数据的内部存储单元。这样就可以随时追踪停电发生了多长时间。这里可作为接口协议使用的尤其是 TCP/IP 协议(传输控制协议 / 互联网协议)或者 PPP 协议(PPP = 点到点协议)。

[0042] 能源市场自由化带来的另一个问题是通过许多节点不加密传输机密的个人数据,因此存在非法人员很容易获知并且滥用数据的风险。DE 10 2006 030 533A1 公开了一种传输、继续处理用量计量装置的信息的方法,在第一个步骤中通过用量计量装置本身采集与用量计量装置有关的所有信息(日期和时间、设备号、当前的用量读数、技术状态、检定有效期、篡改信息、接线条件、温度等等),然后将其处理成可供使用的数字信息。在第二个步骤中通过一个处理模块记录这些信息,然后利用一种数学算法将其编码,以字母形式将其汇编在一份总状态报告之中。处理模块由一个微处理器与一个包含以及保存加密程序的程序单元构成。将编码后的状态报告保存在非易失性存储器之中,可以根据不同的要求以不同的形式将其提供给传输或者处理装置。例如在用量计量装置上按下一个按钮,就能在(LCD)显示屏中看见经过编码的并且自动验证的状态报告,可通过红外接口或者电接口将其输出(通过互联网、无线电、电话(固网、GSM、GPRS、UMTS 等等)以及通过传真或者通过

电力线通信系统 (PLC) 进行传输)。可以在一个用来处理抄表和用量数据采集过程的任务管理和信息系统中将相应用量计量装置的所有基本数据和运动数据进行解密,然后自动按照计划进行使用和处理。

[0043] 在数据处理过程中用作电子身份证明的是电子签名,越来越多的使用数字签名(这是一种加密方法,可将一个数字计算成为一个“消息”,可以通过每一个人检查其来源以及与消息之间的归属关系)。数字签名均基于非对称加密系统,因此均使用一个由(秘密)私钥和(非秘密)公钥组成的密钥对。在德国签名法中将这些密钥称作(私人)签名密钥和(公共)签名验证密钥,或者以英语称作私钥(Private Key)和公钥(Public Key)。在数字签名中通常并不将私钥直接用于消息,而是用于其哈希值,可利用哈希函数(例如SHA-1)从消息算出哈希值。如果已经利用电子证书将公钥对应于某一个人,由于只有一个与该公钥对应的私钥,因此就可以通过认证服务提供者(ZDA)的公共目录,确定或检查认证机构的身份,更高级的认证机构又可以对该认证机构进行认证。一般将能够给数字签名加上时间戳的设备作为时间戳设备。为了给数字签名加上时间戳,主要应将时间戳设备的本地时间与标准时间之差保持在某一个预先规定的阈值范围之内。可以借助其中包含错误标准时间作为标准时间的无线电波适当处理时间戳设备的本地时间,使其超前于或滞后于真实时间。为了防止非授权用户篡改本地时间,例如DE 10 2005 033 162 A1就公开了一种时间戳设备与一种供电机制,这种供电机制不仅可在“非工作模式”期间减小电流消耗,而且也可在将时间戳设备首次切流到准备就绪状态之后在并不使用时间戳设备的“睡眠模式”期间减小电流消耗。但这期间不必将内部时钟发生器终保持在工作状态,并且不必始终接收时间校准信号。其原因在于:可以采用认证密钥在某一预定时间从时间服务器接收标准时间。此外还可使用随机存取存储器(RAM),尤其可使用一种易失性存储器来保存认证密钥,始终将电流提供给RAM以防止非授权用户获得认证密钥。在“非工作模式”期间仅将电流提供给保存认证密钥的易失性RAM。在“工作模式”期间将电流提供给时间戳设备的所有功能单元。其中接收真实时间的单元可使用保存在认证密钥存储单元中的认证密钥对经过加密的真实时间进行解密。按照一种实施方式,时间修改处理器利用无线电波时间修改本地时间,时间修正处理器则在满足预定条件时从时间服务器接收真实时间来修正本地时间。在“睡眠模式”期间利用电源控制器中断时间校准信号接收器与显示单元的电源。如果非授权用户尝试拆除时间戳设备来获得认证密钥,就会中断存储器(RAM)的电源,并且同样也会清除所保存的认证密钥。

[0044] 此外DE 102 04 065 A1还公开了用于验证并且保护用量计量值完整性的一种方法和一种装置。可通过公共网络(例如供电网络和/或者互联网和/或者电话网和/或者GSM网络和/或者UMTS网络)传输所提供的数据集和/或者控制码和/或者身份控制码。通过特殊标志的数据采集仪所采集的数据是电流、燃气、水的用量计量值。除此之外,还适宜将可以设定数据集数量的控制码以可以调出的方式保存在数据采集仪之中,将身份控制码存放在对特别标志的数据采集仪进行验证的检验机构之中。按照该方法的一种实施方式所述,所传输的数据集的完整性控制方法为:重新自动将一个控制码分配给所传输的数据集,与传输之前分配给数据集的控制码一样以相同方式生成需要重新分配的控制码,接着将新生成的控制码与所传输的和/或者与传输之前分配给数据集并且保存在特殊标志的数据采集仪之中的控制码进行比较。具体而言,该装置包括:用来读入数据的构件;一个随

机数生成器；用来接收随机数生成器启用 / 取消控制信号的构件；用来将读入数据与随机数生成器所生成的随机数关联起来的构件；用来计算标识读入数据的控制码的构件，或者用来计算标识与随机数关联的读入数据的控制码的构件；用来输出控制码的构件。此外该装置还包括：至少一个防止或显示非法入侵该装置的保护元件；用来以显示屏形式回放数据的构件；用来保存数据的构件；以及 / 或者用来输入数据存储器访问控制指令的构件；以及 / 或者用来选择回放数据的构件。按照以上 DE 102 04 065 A1 所述用于验证并且保护用量计量值完整性的方法和装置，要么将所传输的计量值保存在计量表之中，或者将相应的控制码保存在计量装置之中。在计量装置的显示屏上仅显示保存在其中的内容。

[0045] 最后 DE 199 30 263 A1 公开了用于在电子医疗植入体与患者状态监视设备之间传输数据的一种方法和一种装置。所述电子医疗植入体可以是例如心脏起搏器、除颤器、心脏复律器或者其它电子操动或控制的植入体。为了提供一种能够使植入体节能工作的方法，始终由第一植入式收发单元、也就是由植入体的收发单元发出一个触发信号，且在发出触发信号之后至少使得第一收发单元在第二段时间之内保持准备接收状态。植入体的第一收发单元的准备接收状态仅仅维持一段时间，且这段时间短于直至下一个触发信号的时段，从而在下一个触发信号之前至少关闭第一收发单元的接收部件尤其是发射部件，这样就不会消耗能量。视接收期与静止期之间的比例而定，这样可以达到显著节能的目的。还可采用外部设备对第一收发单元传输的数据进行第一次可信度检查。可以根据某些条件检查发送数据的某些控制位。之后视传输数据的可信度而定，第一收据将会包含用于控制第一收发单元的第二控制信息。如果所传输的数据缺乏可信度，第二控制信息就会包含通过第一收发单元重新传输数据的第一控制信号。这样就能以有益的方式提高传输安全性，因为可再次请求可能传输失败的数据。进一步提高数据真实性概率的方式为：当所传输的数据可信时，用于控制数据传输的第二收发单元通过植入体至少将一部分所传输的数据回送给第一收发单元。如果这部分数据与所发送的数据不一致，则很可能在传输给第二收发单元时就已出现了错误。植入体最好在检查数据传输之后通过第一收发单元将第二收据发送给第二收发单元。如果确定数据传输成功，第二收据将包含表示传输有效的第一签名。在这次发射之后，植入体至少关闭第一收发单元的准备接收状态，尤其是关闭准备发射状态。重新输出一个触发信号就会标记静止期结束，这样就优化了静止期的持续时间。此外用来进一步提高数据真实性概率的外部设备还可对第二收据进行第二次可信度检查。如果发现第二收据缺少可信度，就会在发送第二收据后的另一个时段结束之后重新查询植入体。在另一个时段结束之后，植入体在另一个时段接收第一收发单元的准备发送信息，该时段足以接收、应答外部设备的请求。此外还以再次发送第二收据和 / 或者上次发送的数据的方式应答请求。这样就能保证使得短暂干扰的影响比较小。此外还可以根据外部设备中重复存在的第二收据和 / 或者上次发送的数据的比较结果，决定是否可以将数据集作为有效。这里最好也可在发现数据传输出错时通过第一收发单元重新传输数据，只要重新传输的次数很少且可避免植入体的电源超负荷即可。可将一种基于私钥 - 公钥系统的 128 位 DES 加密方法用于传输 SMS。可通过软件实现加密，即不使用加密 IC。在这一特殊的医疗应用领域方面，由于从植入体至外部设备的作用距离很短，此外还根据植入体对数据进行了编码，因此不需要再进行加密。

[0046] 从现有技术来看，已知有各种不同的系统可用来抄读计量表数据，当今将这些系

统通常统称为 AMM 系统 (AMM :Automatic Meter Management/ 自动计量管理)。AMM 在很大程度上可替代早已为人所知的 AMR(Automatic Meter Reading/ 自动抄表) (德语也称作 ZFA(远程抄表)), 因为与开头所述数据抄读方式的主要功能相比增加了一些新的特色功能。但这一发展的着眼点是防止最终消费者 / 最终用户非法篡改, 以明确、自动、无干扰且无错误的方式传输用量计量值并且将其对应于相应的用量表, 从而可以据此在相应公共事业公司的结算单位 (结算中心) 开具资费账单。供能公司的这些设备通常均经过适当设计, 以便能够以尽可能简单而且成本低廉的方式采集发生地点 (即最终用户, 例如家庭, 但也包括工业界或者社区) 的用量数据 (资源计量表, 例如电表或者水表), 并且同样也能以尽可能简单而且成本低廉的方式将这些用量数据传输给控制中心 (通信方法), 在控制中心以自动结算方式处理上述最终用户的用量数据。使用者始终是购置资源计量表的供能公司, 供能公司在用户处安装、维护并且抄读这些计量表: 通信装置同样如此。上述在先技术始终将用量表数据传输给结算中心, 以及将可能存在的故障信息 (例如泄漏) 发送给控制中心。但是对于最终用户 (例如家庭用户) 群体不够重视。因此在实践中缺少不仅能够独立于其它现有技术条件普遍应用、而且也能使用户现场自行监控 (用量 / 泄漏等等) 的一种用量表和一种识别篡改的方法。由于计量装置制造行业是进步神速、日新月异的行业, 因此重要的是迅速采取改进和简化措施, 并且将其付诸实施。

发明内容

[0047] 本发明的任务在于, 设计一种能够与至少一个系统进行数据通信的计量装置, 从而能够将该系统所返回的计量数据识别为自己的数据, 并且能够检查是否被篡改。

[0048] 采用权利要求 1 所述的一种计量装置, 即可解决这一任务, 所述计量装置能够与至少一个系统进行数据通信, 能够将该系统通过数据通信返回的计量数据识别为自己的数据, 并且能杜绝篡改计量值, 从而能以可信方式提供这些返回的计量数据供继续处理 / 分析或者显示, 所述计量装置具有:

[0049] • 至少一个与某一系统的组件之间的通信接口, 所述系统至少能够接收经过签名和 / 或者加密的计量值, 能将这些计量值保存在存储器之中, 并且能返回这些计量值, 而且也可相对于某一时间基准提供时间信息,

[0050] • 至少一个计量模块, 该计量模块能将至少一个传感器提供的计量信号对应于能量计量值或者计量表读数,

[0051] • 至少一个用于保存上次测定的能量计量值或者计量表读数 (简称: 计量值) 的存储器,

[0052] • 至少一个时间戳存储器, 用于保存针对上次产生的计量值在时间模块中确定的时间戳,

[0053] • 至少一个时间调整模块, 该模块可检查系统通过通信接口提供的时间, 并且可跟踪时间模块中的本地时间,

[0054] • 至少一个用于保存分配给计量装置的标识符的存储器,

[0055] • 至少一个用于加密和 / 或者签名密钥的存储器,

[0056] • 至少一个加密和 / 或者签名编码器, 该编码器通过使用密钥存储器中的密钥, 将用来检查数据完整性的信息配备给提供给上述存储器的包括有效标记和可信标记在内的

信息，一个当前的数据集中进行组合，然后至少将其交给通信接口进行传输，仅将一部分先前的数据集或者其内容保存在计量装置之中，以及

[0057] • 至少一个加密和 / 或者签名解码器，该解码器可通过使用密钥存储器中的密钥检查对通过通信接口提供的具有计量值的数据集进行检查以确定数据内容的完整性以及计量装置的标识符，并且在检查结果为肯定的情况下提供这些数据供继续处理 / 分析或者显示。

[0058] 按照本发明所述，还可采用权利要求 6 所述的一种方法解决这一任务，所述方法可用来识别对某一经过认证和 / 或者检定的计量装置的非法篡改，按照所述的方法：

[0059] • 生成至少包含标识符、时间值、计量值和签名的数据包，

[0060] • 将这些数据包传输给未经认证和 / 或者检定的某一个系统或者该系统的组件，这些系统组件可保存这些数据包或者相关部分，并且可根据计量装置的请求将这些数据包或者相关部分返回给计量装置，

[0061] • 在此期间，数据包或者其内容不保存在计量装置中，

[0062] • 计量装置可以安全性得到证实的方式根据密钥和签名，检查系统或者系统组件所提供的数据包或者其相关内容，检查数据包的数据是否未被更改并且来自于该计量装置，

[0063] • 在经过检定认证的显示器上以与没有离开计量装置的计量值相同的可信状态显示经过成功验证的数据。

[0064] 与在先技术相比，本发明所述的计量装置以及本发明所述的方法具有过程比较简单而且成本较低的优点，因为数据可以保存在未经认证的设备或系统之中，例如网络运营商计算中心的计量值数据库。另一个优点在于，还可以将值对（即计量表读数和时间戳）用于制定下游的费率，从而也能够例如在账单上一并输出相应的值对。用户尤其可以利用简单的辅助手段（例如按下计量表上的按钮来翻阅计量值）直接检查值对的正确性，不必显示传输给网络运营商的所有计量值的清单，也不必查找与账单相关的数据。计量装置可生成许多计量数据（例如每 15 分钟包含一个值的计量表读数曲线），将这些数据传输给上位系统。下游费率可根据与用户签订的合同决定哪些值现在与结算相关，并且在账单上一并输出（以纸页形式打印出来）。计量表仅显示所使用的值就足以检查结算值 - 甚至比例如从每天 96 个值中找出 2 ~ 4 个相关的值还要方便。按照本发明所述很容易实现这一点，因为上位系统可根据用户请求（例如按下计量表或者通信模块上的按钮）仅返回所使用的结算值，并且可在这些值中往后翻阅。计量表可以通过现有签名确定在其显示屏上仅显示没有篡改的值，尽管这些值并没有保存在计量装置之内。因此本发明所述的计量装置更加简单，因为计量装置不必包含计量值存储器或者控制码存储器。另一个优点在于，用于可以信赖计量表，因为可通过 PTB 或者类似的组织保证仅仅显示有效而且正确的数据（源自于经过检定的计量装置 / 计量表部件的数据）。

[0065] 按照本发明权利要求 2 所述的一种首选实施方式，计量装置具有一个用户接口，可通过该接口将已经检查过数据内容和标识符完整性的数据集传输给用户的任意一台合适的设备，该设备具有自身的显示器或者用来转发给具有显示器的设备。

[0066] 本发明这种实施方式的优点在于：用户可以通过计量表上现有的、并且同样也经过联邦物理技术研究所 PTB 验证的用户接口，利用自己自由选择的设备（例如具有 USB 通

用串行接口的读取头和经销商的 PC 软件) 直接抄读经过检验的数据, 并且可以对其进行继续处理。

[0067] 按照本发明权利要求 5 所述的改进实施方式, 使用世界协调时 UTC 尤其是(德国)联邦物理技术研究所的 UTC(PTB) 作为世界基准。

附图说明

[0068] 关于本发明的其它优点和细节描述, 可参阅以下参考附图对本发明的首选实施方式所作的说明。附图所示如下:

[0069] 附图 1 设计成计能表形式的计量装置的方框图,

[0070] 附图 2 附图 1 所示计能表的设计流程图, 该实施方式没有按钮, 使用两个光接口,

[0071] 附图 3 附图 1 所示计能表的设计流程图, 本实施方式有按钮, 并且在通信模块上使用光接口,

[0072] 附图 4 附图 1 所示计能表的设计流程图, 通过用户接口或者显示器输出验证后的数据, 以及

[0073] 附图 5 连接本发明所述计能表的不同实施方式。

具体实施方式

[0074] 附图 1 所示为本发明所述计量装置 EZ 的一种首选实施方式的方框图, 用户很容易操作该计量装置, 无需具备电子数据处理知识。以下是将本发明所述解决方案用于计能表 EZ 的设计说明, 也可将本发明所述的计量装置 EZ 和方法用于具有相应接口的其它设备, 例如可用来检测太阳能设备馈入到供电网络中的电能。

[0075] 其原因就在于本发明所述的方案基于可配置特性, 能够独立于设备统一进行误差处理, 并且很容易根据相应的现有条件进行调整, 无需修改本发明或基本设计方案即可进行整合。除了采集计量值、计数的主要功能之外, 该系统还可对外通信。该通信功能可以包含不同的接口, 尤其是用来抄读数据的接口 KSS, 例如可以远程抄读那些主要通过供能公司 EVU 结算电能的数据, 另一方面还可以包含用于监视用量和检查 EVU 账单的用户接口 KSK。本发明涉及不同型式的接口, 例如通过 PLC、GPRS 与 EVU 进行通信的接口, 或者组合运用多种通信技术。可以将用户接口 KSK 设计成显示屏 A 或者 PC 接口, 或者也可采用其它通信技术将数据提供给用户设备 KG, 例如使用 USB 记忆棒。

[0076] 附图 1 所示的计能表 EZ 能够与至少一个系统进行数据通信, 能够将系统通过数据通信功能返回的计量数据识别为自己的数据, 并且能杜绝篡改计量值, 从而能在自己的显示器 A 上以可信方式显示所返回的计量数据。为此计能表 EZ 具有至少一个与某一系统的组件 SK 之间的通信接口 KSS, 所述系统至少能够接收经过签名和/或者加密的计量值, 能将这些计量值保存在存储器 SM 之中, 并且能返回这些计量值, 而且也可相对于某一时间基准 ZR 提供时间信息。尤其可以通过联邦物理技术研究所 PTB 设立在不伦瑞克(Braunschweig)的 NTP 服务器获得时间基准 ZR。计量装置 / 计量表 EZ 适宜由两个模块构成, 即一个计量模块 M 和一个传感器模块 S。所述计量模块 M 将能量计量值或计量表读数对应于传感器模块 S 所提供的计量信号。此外还采用了以下存储器: 至少一个存储器 MS, 用于保存上次测定的能量计量值或者计量表读数(简称为:计量值); 至少一个时间戳存储器 ZS, 用于保存

针对上次产生的计量值在时间模块 Z 中确定的时间戳 ; 至少一个时间调整模块 ZA , 可检查系统通过通信接口 KSS 提供的时间基准 ZR , 并且可跟踪时间模块 Z 中的本地时间 ; 至少一个用于保存分配给计量装置 / 计能表 EZ 的标识符的存储器 IS ; 以及至少一个用于加密和 / 或者签名密钥的存储器 SS 。适宜将序列号或者系统运营商的资产编号保存在标识符存储器 IS 之中。此外计能表 EZ 还具有至少一个与存储器 SS 、 IS 、 MS 、 ZS 相连的加密和 / 或签名编码器 VSK , 该编码器通过使用密钥存储器 SS 中的密钥 , 将用来检查数据完整性的信息提供给标识符存储器 IS 、计量值 / 计量表读数临时存储器 MS 和时间戳存储器 ZS 中提供的包括有效标记和可信标记在内的信息 , 在一个 (当前的) 数据集中进行组合 , 并且将其至少交给通信接口 KSS 进行传输。也可以将不同的有效和可信标记组合为一个状态字。按照本发明所述 , 先前的数据集或者其内容 (例如最近五个之前的数据集) 并不保存在计量装置 EZ 之中。最后还有至少一个加密和 / 或签名解码器 VSD , 该解码器可通过使用密钥存储器 SS 中的密钥对通过通信接口 KSS 提供的具有计量值的数据集进行检查以确定数据内容的完整性以及计量装置 (EZ) 的标识符 , 并且在检查结果为肯定的情况下在显示器 A 上显示这些数据。至少还有一个包括程序存储器 (附图中没有绘出) 的控制装置 , 用以控制显示屏 A 上的输出、分析控制信号、操作某一个按钮 (附图中没有绘出) 或者保存经过同步的本地时间、增大或者减小当前的循环时间等等。

[0077] 本发明所述的计量装置 / 计能表 EZ 还具有一个用户接口 KSK , 可通过该接口将已经检查过数据内容和标识符完整性的数据集或数据包传输给用户的任意一台合适的设备 KG , 该设备具有自身的显示器 KA 或者可用来转发给具有显示器的设备。在附图 1 中以箭头线表示在显示器 A 或者通过用户接口 KSK 进行输出 , 箭头线起始于加密和 / 或者签字解码器 VSD , 该解码器与通信接口 KSS 和密钥存储器 SS 相连。

[0078] 时间模块 Z 用于控制本地时间和日期 , 可以使用世界协调时 UTC 尤其是 (德国) 联邦物理研究所的 UTC(PTB) 作为世界基准 ZR , 并且可以使用网络时间协议 NTP 通过公共网络将系统的时间基准 ZR 传输给计量装置 / 计能表 EZ 。为此将时间模块 Z 与时间调整模块 ZA 相连 , 该时间调整模块又与通信接口 KSS 相连。附图 1 中的虚箭头线表示将时间戳 ZS 添加给最后一次在加密和 / 或者密钥编码器 VSK 中生成的计量值 (计量模块 M 或存储器 MS) ; 通过始于计量模块 M / 时间模块 Z 直至显示器 AA / 用户接口 KSK 的实心粗箭头线表示相同的情况。

[0079] 如附图 2 ~ 5 所示 , 计能表 EZ 一方面通过接口 KSS 进行通信 , 用以远程抄读主要通过供能公司 EVU 结算电能的数据 ; 另一方面通过用户接口 KSK 进行通信 , 用以在逻辑和物理层监测用量以及检查 EVU 的账单。从本地数据库或者 (如果通信功能强大) 从远程数据库获取数据 (网络或者计量点运营者 RZ , 参见附图 5) 。按照本发明所述 , 不需要使用公钥来检查数据 (公钥长度例如为 192 个比特 = 24 个二进制字节 (Byte bin) = 48 个十六进制字符) , 而是可以使用现有的签名方法和私钥。其原因在于接口 (KSS) 在计量表 EZ 上 , 因此 EVU 无法对其施加影响 , 从而可以向外转发数据 , 无需设置或者传输公钥。这样无需将公钥分配给用户 , 就能迅速构建一个允许用户以简单手段检查结算用数据的系统 ; 例如按压计量表上的按钮 (往后翻阅) , 也可以将无法篡改的数据传输给显示屏或者用户的 PC (参见附图 1 中的 KG) 。这样计量装置 / 量表 EZ 就能通过接口 KSS 接收计量值 , 检查计量值是否源自于计量表并且没有被篡改 , 并且在显示器 A 上显示计量值 , 也就是已经离开计量表区

域的数据（必须检定的部件 - 计量板）。另一个优点在于，也可以将本发明所述的方案从短信语言 SML（智能消息语言 :Smart Message Language）扩展为设备语言报文规范 DLMS（设备语言报文规范 :Device Language MessageSpecification）。

[0080] 附图 2 所示为附图 1 所示计能表的设计流程图，该实施方式没有按钮，使用两个光接口 (KSS)。按照本发明所述，可生成由（存储器 IS 中的）标识符、（存储器 MS 中的）计量值和（存储器 ZS 中的）时间戳组成的 SML 消息，利用 ECC192 方法生成该消息的签名（签名长度为 192 位的椭圆曲线加密码），然后通过光接口 KSS 传输消息。按照本发明所述，采用以下功能 / 组件：

- [0081] • 时间模块 Z，
- [0082] • 接收用于调整始终时间的 SML 消息，
- [0083] • 可靠保存用于生成签名的私钥 (EVU 无法读出)，
- [0084] 并且可以选配：
 - [0085] • 能够显示日期、计量值和时间的显示器 / 显示器 A。

[0086] 按照本发明所述，计量装置 / 计能表 EZ 能够接收 SML 计量值消息，可以检查签名的有效性，并且能确认该三元变量（标识符、计量值和时间戳）是否源自于计量装置以及是否已被更改。按照本发明所述，只能在这种情况下在显示屏 A 上将该值显示一定的时间（例如 20 秒）。

[0087] 这样就能根据请求（例如按下调制解调器上的按钮）向用户显示结算数据。由于计量装置 / 计能表 EZ 仅显示经过其签名的值，因此杜绝了计量点运营者、网络运营者或者电力供应者篡改数据。与在先技术相比，本发明所述的计量装置以及本发明所述的方法尤其具有过程比较简单而且成本较低的优点，因为可以将数据保存在未经认证的设备或系统之中（并且在此期间不将数据包或者其内容保存在计量装置 / 计能表 EZ 之中）。通过检定机构保证用户信任显示器 A 以及计量表 EZ 的用户接口 KSK。在安装本发明所述的计量装置 / 计能表 EZ 时，不需要以信封转交“公钥”的方式管理用于生成签名的密钥，这与在先技术相比明显便于使用（无需管理密钥）。

[0088] 附图 3 所示为附图 1 所示计量装置 / 能表 EZ 的设计流程图，在该实施方式中有按钮并且使用光接口连接到通信模块。将按钮置于计量装置 / 计能表 EZ 之中，可提高用户对显示屏 / 显示器 A 所显示的数据的信任。按下该按钮，计能表 EZ 就会通过后端 / 内部接口请求过去的计量值。现在可以通过一个内置通信模块应答该请求，例如 DLC 模块（配电线载波，申请人的电力线通信模块）、外部调制解调器、MUC（公用事业通信系统，例如参见 FNN(VDE 中的网络技术 / 网络运营论坛) 的需求规格说明书 MUC(目前版本 0.60)），或者通过数据库服务器的另一个通信功能应答该请求。如附图 2 所示，计量表(**Zähler**) EZ 检查应答，并且仅当计量表 EZ 能够通过签名 / 密钥证实这些值均源自于计量表而且没有被篡改时才会显示应答。这样不仅可任意安装按钮，而且也可任意安排数据的保存位置，并且不属于计量装置 / 计量表 EZ 的认证范畴。

[0089] 附图 4 所示为附图 1 所示计量装置 / 计能表的设计流程图，通过用户接口或者显示器输出验证后的数据。该实施方式使得用户能够利用抄读电缆将标准显示屏 A 或者 PC 软件连接到用户接口 KSK（以下称作抄读单元 KG，通过可信赖的货源采购，例如消费者保护组织或者建筑市场），无需输入密钥，即可抄读经验证的数据。为此可通过计量装置 / 计能表

EZ 的内部 / 后端接口将抄读单元 KG 的请求转发给通信模块 DLC 板卡或者 MUC。检查这些模块的应答，并且仅当计量表 EZ 能够确认真实性时才会转发。这样就只能在用户接口 KSK 之外篡改数据。但由于所有相关组件完全在用户手中，因此可以对此加以信任。

[0090] 附图 5 所示为连接本发明所述计量装置 / 计能表 EZ 的不同实施方式示意图。按照上图所示的实施方式，计量装置 / 计能表 EZ 通过通信接口 KSS、导线 L(例如 LAN 局域网络)、调制解调器 / 路由器 R、连接 W(WAN 广域网络 ;DSL, 电力线等等) 与网络或计量点运营者的计算中心 RZ 中用于经过签名的计量值（也就是说在 RZ 中完全智能化）和时间基准 ZR(例如联邦物理技术研究所 PTB 设立在不伦瑞克的 NTP 服务器) 的存储器 SM 或数据库 DB 相连。

[0091] 按照附图 5 中图所示的实施方式，计量装置 / 计能表 EZ 在近距范围内通过网络 L 与公用事业通信系统 MUC 相连，该通信系统将一部分经过签名的计量值（例如先前的或上一个的计量值）暂时保存在存储器 SM2 之中，而用户 / 计能表 EZ 的另一部分经过签名的值则保存在存储器 SM1 或者网络或计量点运营者 RZ 的数据库 DB 之中。此外还可以利用一个通过连接导线 V 和外部网络 (IP, 互联网) 或 WAN 连接 (GSM、GPRS、ISDN、电力线等等) 与网络或计量点运营者的中央装置 RZ 相连的切断装置 AE 遥控切断电力供应或者（例如家庭自动化领域的）遥控装置 / 设备。

[0092] 按照附图 5 下图所示的实施方式，“智能”计量装置 / 计能表在法定检定部分中具有一个计量装置 / 计能表 EZ，并且在不需要认证的部分中具有一个通信 / 控制模块 COM 或者一个 MUC(例如具有用于一部分经过签名的计量值的存储器 SM2)。所述计量装置 / 计能表 EZ 和 COM/MUC 均布置在同一个外壳之中。其它计量装置 / 计能表可以通过近距范围内的连接或网络 L(例如 M 总线、无线 M 总线、DECT、ZIGBEE(作用距离较短用于传感器无线联网的无线标准) 、蓝牙、Konnex 、传感器网络或者现场总线) 与 COM 或者 MUC 相连，通过 WAN 、 IP 将用户 / 计能表 EZ 的一部分经过签名的值传输给存储器 SM1/ 网络或计量点运营者 RZ 的数据库 DB 并且保存在这里。可以通过导线（例如电力线）在中央计算机 RZ 与通信 / 控制模块 / 终端设备 COM 之间交换数据，或者使用一种互联网协议或者不同的协议 (Windows NT 、 Linux 、 Unix 计算机网络协议，或者例如 SMS 或 WAP 手机协议等等) 以无线方式交换数据。这样也能集中上载新的功能（例如新的费率切换时间）、实现路由功能，或者以无线方式远程抄读家庭计量表，在网页上访问个人用电量。

[0093] 本发明并非仅限于附图所示以及所描述的实施例，也包括作用与本发明相当的所有实施形式。本发明所述的计量装置也可用于本申请人的欧洲专利申请书 EP 1 850 500 A1 涉及的对象，控制装置除了具有控制功能之外，也可承担通信功能 (MUC/COM) ，方法是使其具有至少一个“准专用的”通信控制器，该通信控制器具有至少一个可以自由编程的通信算术逻辑单元 ALU，因此控制装置的中断延迟时间并不用来直接同步某一硬件组件的控制功能（例如电机的定位控制）；可以按照一种与相应制造商 / 用户约定的协议，通过推模式在轮询接口上提供上报数据；在消息中显示缺少有效时间，例如对用户没有害处的特殊费率，可以通过软件实现时间模块 Z，并且不必采用具有失效容限的实时时钟 RTC；可以将“安防”服务连接到附图 5 下图所示的“智能”计量装置 / 计能表，例如入侵传感器、门禁和打卡器、视频监视系统等等，连接住宅和楼宇管理系统的功能，例如卷帘门和照明控制器以及家用电气的控制与监视（关键字：家庭自动化），或者连接自动化技术设备的辅助功能，例如

电梯和其它电气系统的控制与监视等等。

[0094] 此外,本发明也不限于权利要求1或6中所定义的特征组合,而是可以对所公布的所有单一特征中的某些特征进行任意组合。这就意味着,原则上可以省略权利要求1或6所述的每一个单一特征,或者将其替换成本发明申请书另一部分中所公布的至少某一个单一特征。

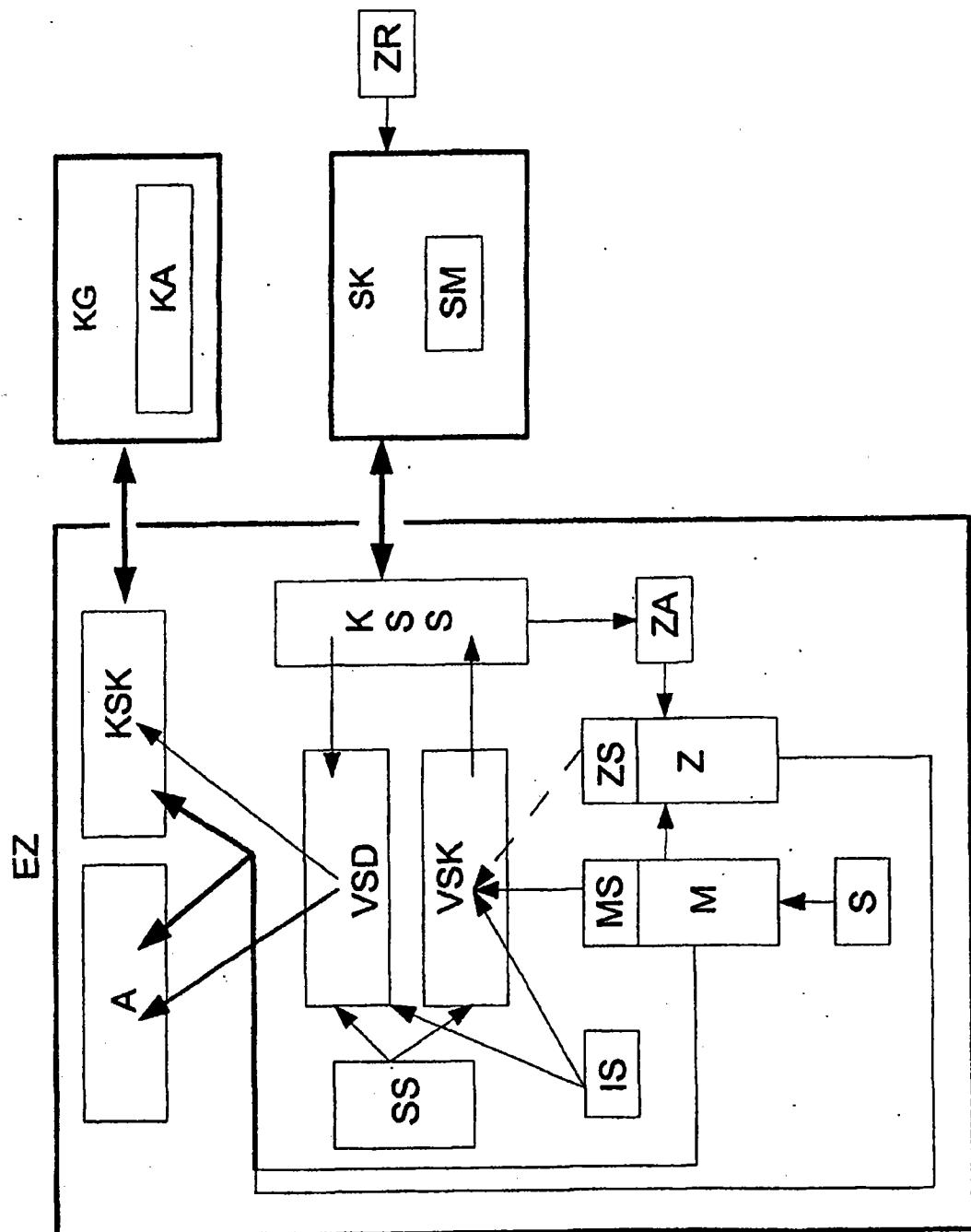


图 1

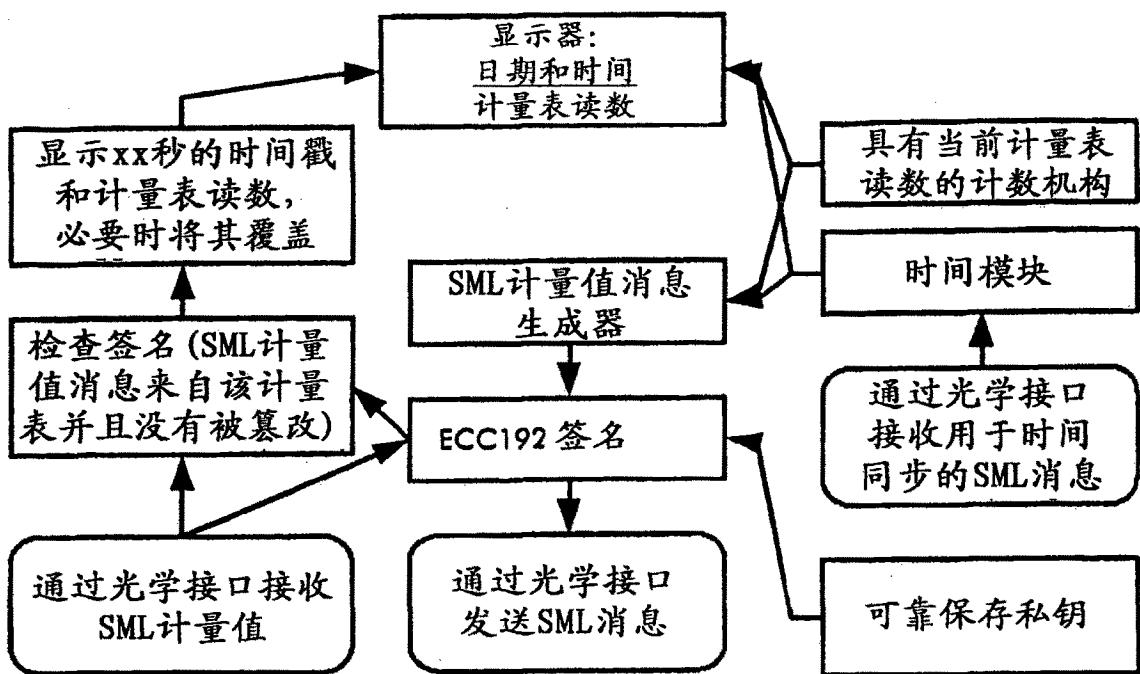


图 2

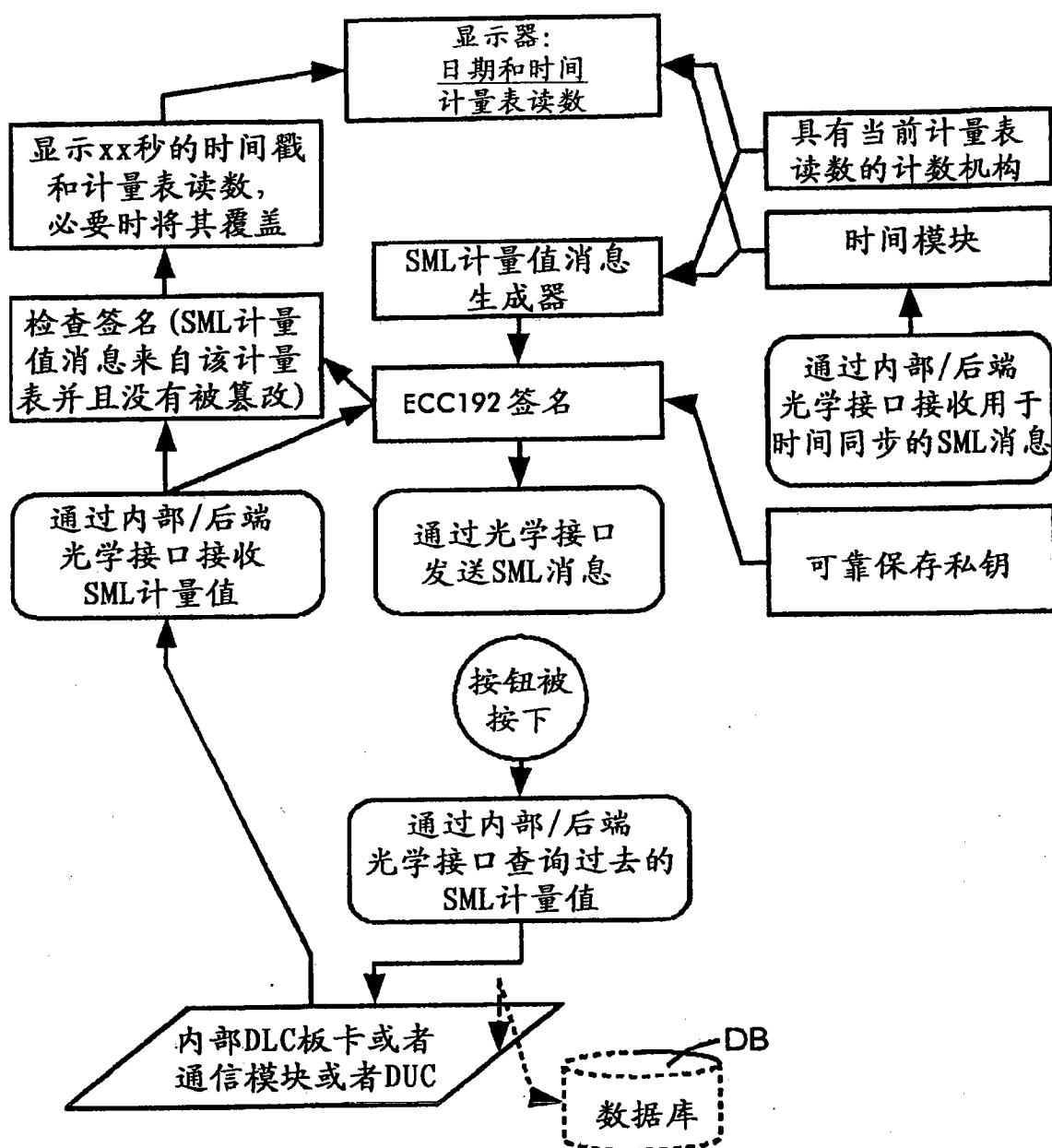


图 3

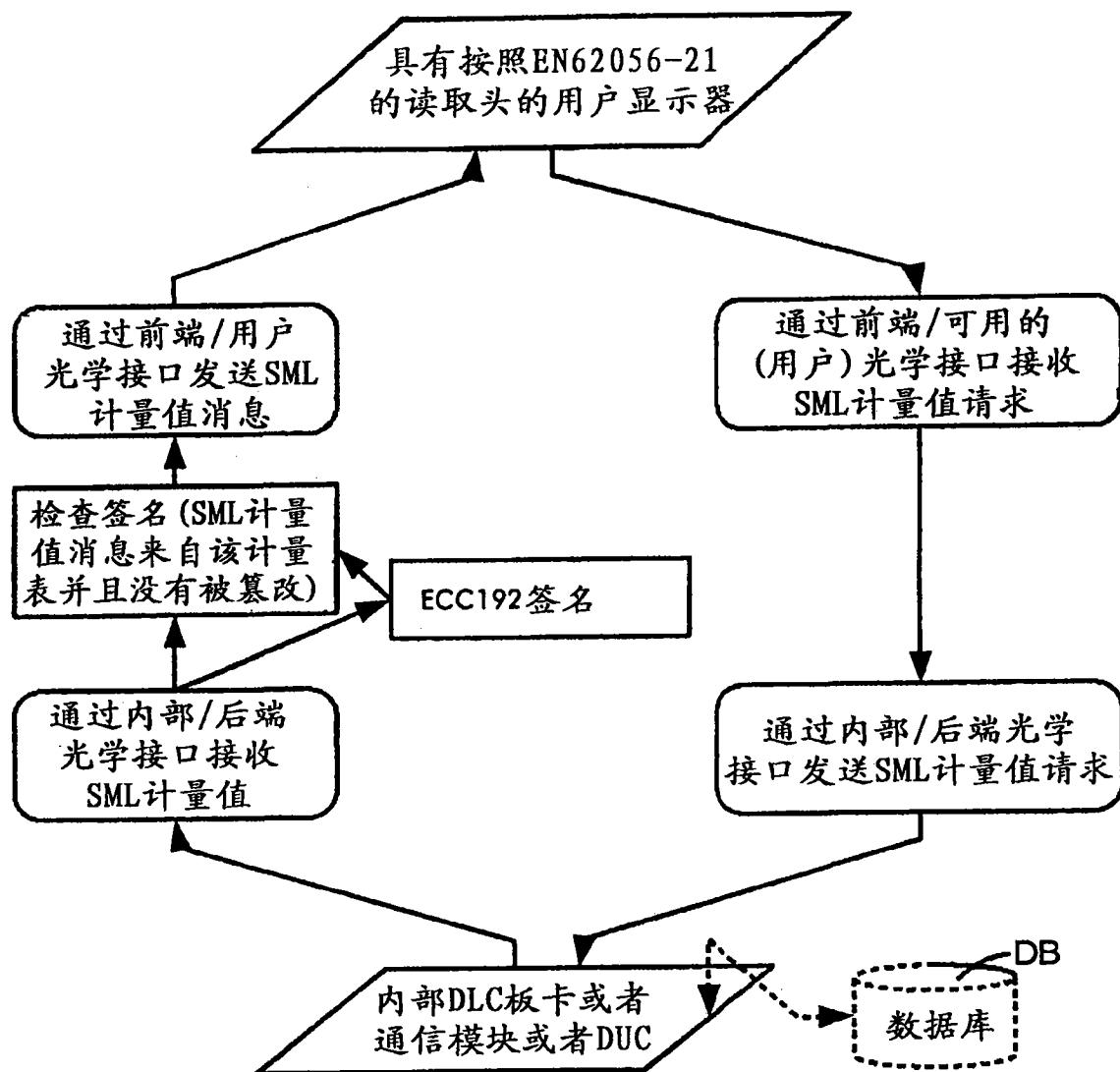


图 4

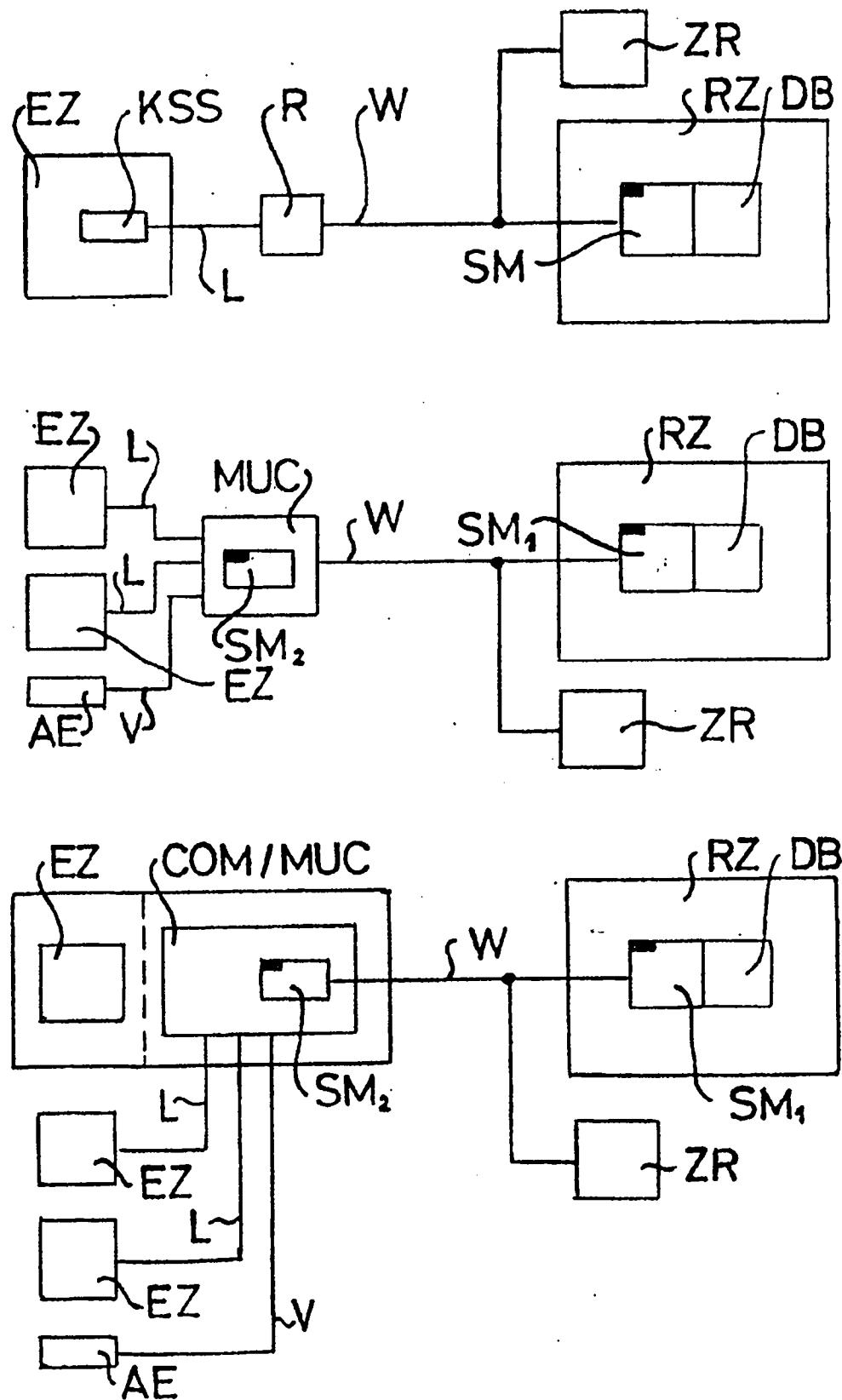


图 5