

1. 一种远控智能水表信息安全管理模块,其特征在于:所述信息安全管理模块包括处理器、第一数据接口、第二数据接口与 FLASH 存储器,所述处理器分别接入第一数据接口、第二数据接口与 FLASH 存储器,其中:

所述第一数据接口用于执行远控智能水表与数据传输模块的唯一数据通信,并在接收到来自于数据传输模块的外部数据时将其传输至处理器;所述数据传输模块直接接收来自于远程售水管理系统的外部数据;

所述 FLASH 存储器用于存储信息安全管理模块中的控制及文件管理程序;

所述第二数据接口用于执行处理器与远控智能水表终端主控制器之间的数据通信,所述远控智能水表终端主控制器用于按照处理器的指令执行相应的表端操作;

所述处理器用于在接收到来自于第一数据接口的外部数据时,对发送外部数据的售水管理系统进行身份认证,判断是否获取该外部数据中的加密数据包,并根据数据中包含的事务通过第二数据接口向远控智能水表终端主控制器发送相应的操作指令。

2. 根据权利要求 1 所述的远控智能水表信息安全管理模块,其特征在于:所述处理器用于在接收到来自于第一数据接口的外部数据时,根据外部数据对售水管理系统进行身份认证,当认证结果判断为合法时,则对加密数据包进行解密及完整性校验,反之则复位初始状态;

数据完整性校验通过后,对数据的有效性进行验证,反之则复位初始状态;

数据有效性验证通过后,对数据中包含的事务进行预处理,并通过第二数据接口从远控智能水表终端主控制器中获取相应的返回信息,将所述返回信息加密后通过第一数据接口返回给数据传输模块,当得到有效确认后则将预处理结果予以认可且储存相关的操作信息,并向远控智能水表终端主控制器发送操作指令;反之则放弃预处理结果或作缓存处理。

3. 根据权利要求 1 或 2 所述的远控智能水表信息安全管理模块,其特征在于:所述 FLASH 存储器内预置有协议限制条件与多个不同的密钥程序,用于在信息安全管理模块分别与售水管理系统中不同分级的子系统进行数据交换时,处理器根据外部数据的加密密钥与 FLASH 存储器中预置的多个密钥程序相比较,从而认证售水管理系统的身份,并在加密数据包解密及完整性校验通过后,根据协议限制条件验证数据在当前身份下的有效性,判断是否对数据中的事务进行预处理;

所述第一数据接口还接入 IC 卡信息交换模块,用于在接收到来自于 IC 卡信息交换模块的外部数据时将其传输至处理器,处理器对所述外部数据执行与来自于数据传输模块的外部数据相同的校验。

4. 根据权利要求 1 或 2 所述的远控智能水表信息安全管理模块,其特征在于:所述的信息安全管理模块中还包括 EEPROM 存储器,所述 EEPROM 存储器也接入处理器,用于存储处理器对远控智能水表终端主控制器的相关操作信息,以及处理器对外部数据中事务的预处理结果。

5. 根据权利要求 1 或 2 所述的远控智能水表信息安全管理模块,其特征在于:所述处理器为可执行加密算法的中央处理器或单片机;所述数据传输模块为网络通信模块或总线通信模块。

6. 根据权利要求 1 或 2 所述的远控智能水表信息安全管理模块,其特征在于:所述的第一数据接口为网络通信接口或总线接口。

7. 根据权利要求6所述的远控智能水表信息安全管理模块,其特征在于:所述网络通信接口至少为RF模块接口、Zigbee模块接口、WiFi模块接口、蓝牙模块接口、红外线模块接口或光纤传输接口、数据线传输接口、电力线传输接口当中的任意一种;所述总线接口至少为Mbus总线接口、RS485总线接口、CAN总线接口当中的任意一种。

8. 根据权利要求1或2所述的远控智能水表信息安全管理模块,其特征在于:所述的第二数据接口至少为USART串行接口、SPI串行接口或I2C串行接口当中的任意一种。

9. 根据权利要求1或2所述的远控智能水表信息安全管理模块,其特征在于:所述的信息安全管理模块还包括加密模块,所述加密模块接入处理器,用于对信息安全管理模块与售水管理系统、远控智能水表终端主控制器数据交换的多级加解密,并辅助处理器获取售水管理系统的数据加密密钥进行身份认证。

10. 根据权利要求9所述的远控智能水表信息安全管理模块,其特征在于:所述的加密模块通过AES或3DES的方式进行数据加解密。

远控智能水表信息安全管理模块

技术领域

[0001] 本发明涉及一远控智能水表管理辅助装置,更具体的说,本发明主要涉及一种远控智能水表信息安全管理模块。

背景技术

[0002] 目前,市场上的远控智能水表的品种不是很多,远控智能水表的技术发展处于初级阶段,在有线传输技术,无线传输技术,售水管理系统等等方面的安全性保障还不成熟,不完善,而另一方面远控智能水表需要实时、安全、有效的与自来水公司的主站售水管理系统进行数据交换,因此远控智能水表及其售水管理系统都存在失控的风险。

[0003] 有线通信方式,主要采用光纤传输、数据线传输及电力线传输等方式,这些传输方式都需要布置复杂的线缆,在特殊的地理环境中这些布线会变得相当困难,当线缆出问题或者被人改接后,数据传输的安全性得不到保证。无线通信方式,主要采用 RF 模块、Zigbee 模块、WiFi 模块及蓝牙模块等进行传输,这些无线设备在传输过程中容易受到环境干扰,造成数据交换错误,当出现人为破坏时,数据可能被截获、修改,数据传输的安全性得不到保证。另外自来水公司的售水管理系统尚处于初级阶段,且包含多个子系统,多个子系统都需要与主系统进行数据交换,这些子系统往往会出现数据传输错误,造成远控智能水表与售水管理系统的数据传输的安全性得不到保证。

[0004] 在出现上述的数据传输安全性得不到保证的情况下,在远控智能水表终端主控制器中没有有效的数据验证手段时,外部数据发送端的身份得不到核实,数据得不到有效校验,造成远控智能水表和主站售水管理系统失控,因此有必要在远控智能水表中加装一种信息安全管理的管理辅助装置,实现信息安全管理。

发明内容

[0005] 本发明的目的之一在于针对上述不足,提供一种远控智能水表信息安全管理模块,以期望解决现有技术中各种类型的远控智能水表及其管理系统的信息安全管理得不到保证等问题,从而消除自来水公司运营中信息安全管理风险。

[0006] 为解决上述的技术问题,本发明采用以下技术方案:

[0007] 本发明所提供的一种远控智能水表信息安全管理模块,所述信息安全管理模块包括处理器、第一数据接口、第二数据接口与 FLASH 存储器,所述处理器分别接入第一数据接口、第二数据接口与 FLASH 存储器,其中:

[0008] 所述第一数据接口用于执行远控智能水表与数据传输模块的唯一数据通信,并在接收到来自于数据传输模块的外部数据时将其传输至处理器;所述数据传输模块直接接收来自于远程售水管理系统的外部数据;

[0009] 所述 FLASH 存储器用于存储信息安全管理模块中的控制及文件管理程序;

[0010] 所述第二数据接口用于执行处理器与远控智能水表终端主控制器之间的数据通信,所述远控智能水表终端主控制器用于按照处理器的指令执行相应的表端操作;

[0011] 所述处理器用于在接收到来自于第一数据接口的外部数据时,对发送外部数据的售水管理系统进行身份认证,判断是否获取该外部数据中的加密数据包,并根据数据中包含的事务通过第二数据接口向远控智能水表终端主控制器发送相应的操作指令。

[0012] 作为优选,进一步的技术方案是:所述处理器用于在接收到来自于第一数据接口的外部数据时,根据外部数据对售水管理系统进行身份认证,当认证结果判断为合法时,则对加密数据包进行解密及完整性校验,反之则复位初始状态;

[0013] 数据完整性校验通过后,对数据的有效性进行验证,反之则复位初始状态;

[0014] 数据有效性验证通过后,对数据中包含的事务进行预处理,并通过第二数据接口从远控智能水表终端主控制器中获取相应的返回信息,将所述返回信息加密后通过第一数据接口返回给数据传输模块,当得到有效确认后则将预处理结果予以认可且储存相关的操作信息,并向远控智能水表终端主控制器发送操作指令;反之则放弃预处理结果或作缓存处理。

[0015] 更进一步的技术方案是:所述 FLASH 存储器内预置有协议限制条件与多个不同的密钥程序,用于在信息安全管理模块分别与售水管理系统中不同分级的子系统进行数据交换时,处理器根据外部数据的加密密钥与 FLASH 存储器中预置的多个密钥程序相比较,从而认证售水管理系统的身份,并在加密数据包解密及完整性校验通过后,根据协议限制条件验证数据在当前身份下的有效性,判断是否对数据中的事务进行预处理;

[0016] 所述第一数据接口还接入 IC 卡信息交换模块,用于在接收到来自于 IC 卡信息交换模块的外部数据时将其传输至处理器,处理器对所述外部数据执行与来自于数据传输模块的外部数据相同的校验。

[0017] 更进一步的技术方案是:所述的信息安全管理模块中还包括 EEPROM 存储器,所述 EEPROM 存储器也接入处理器,用于存储处理器对远控智能水表终端主控制器的相关操作信息,以及处理器对外部数据中事务的预处理结果。

[0018] 更进一步的技术方案是:所述处理器为可执行加密算法的中央处理器或单片机;所述数据传输模块为网络通信模块或总线通信模块。

[0019] 更进一步的技术方案是:所述的第一数据接口为网络通信接口或总线接口。

[0020] 更进一步的技术方案是:所述网络通信接口至少为 RF 模块接口、Zigbee 模块接口、WiFi 模块接口、蓝牙模块接口、红外线模块接口或光纤传输接口、数据线传输接口、电力线传输接口当中的任何一种;所述总线接口至少为 Mbus 总线接口、RS485 总线接口、CAN 总线接口当中的任何一种。

[0021] 更进一步的技术方案是:所述的第二数据接口至少为 USART 串行接口、SPI 串行接口或 I2C 串行接口当中的任何一种。

[0022] 更进一步的技术方案是:所述的信息安全管理模块还包括加密模块,所述加密模块接入处理器,用于对信息安全管理模块与售水管理系统、远控智能水表终端主控制器数据交换的多级加解密,并辅助处理器获取售水管理系统的加密密钥进行身份认证。

[0023] 更进一步的技术方案是:所述的加密模块通过 AES(密码学中的高级加密标准,英文 Advanced Encryption Standard 的简称)或 3DES(三重数据加密算法,英文 Triple Data Encryption Algorithm)的方式进行数据加解密。

[0024] 与现有技术相比,本发明的有益效果之一是:信息安全管理模块在通过数据传输

模块与售水管理系统进行数据交换时进行身份认证,保证了两者通信的合法性,远控智能水表终端主控制器必须通过信息安全管理模块才能与外部进行通信;利用不同的密钥可实现自来水公司分级管理的权限设置,且采用 3DES/AES 多级加密方式,使得密钥的安全性较高,并可通过信息安全管理模块上的程序下载口实时升级密钥,避免密钥泄漏所带来的风险;通过内置的数据校验程序,保证传输的数据真实、准确、完整。同时本发明所提供的一种远控智能水表信息安全管理模块结构简单,可嵌入各种类型的远控智能水表中,通过多种通信传输技术与总线接口兼容远控智能水表终端主控制器,并无缝接入供水管理系统,实现远控智能水表分散制造,统一管理,应用范围广阔,且保证自来水公司在终端水表控制上的独立性,且不受外界的制约。

附图说明

[0025] 图 1 为用于说明本发明实施例中的信息安全管理模块结构框图;

[0026] 图 2 为用于说明本发明实施例中的信息安全管理模块应用框图;

[0027] 图 3 为用于说明本发明实施例中的管理系统框图。

具体实施方式

[0028] 下面结合附图对本发明作进一步阐述。

[0029] 参考图 1 所示,本发明的一个实施例是一种远控智能水表信息安全管理模块,所述信息安全管理模块包括处理器、第一数据接口、第二数据接口与 FLASH 存储器,所述处理器分别接入第一数据接口、第二数据接口与 FLASH 存储器,其中:

[0030] 上述第一数据接口的作用是执行远控智能水表与数据传输模块的唯一数据通信,并在接收到来自于数据传输模块的外部数据时将其传输至处理器;所述数据传输模块直接接收来自于远程售水管理系统的外部数据;

[0031] 上述 FLASH 存储器的作用是存储信息安全管理模块中的控制及文件管理程序;

[0032] 参考图 2 所示,上述第二数据接口的作用是执行处理器与远控智能水表终端主控制器之间的数据通信,而远控智能水表终端主控制器的作用是按照处理器的指令执行相应表端操作;

[0033] 上述处理器的作用是在接收到来自于第一数据接口的外部数据时,对发送外部数据的售水管理系统进行身份认证,判断是否获取该外部数据中加密数据包,并根据数据中包含的事务通过第二数据接口向远控智能水表终端主控制器发送相应的操作指令。

[0034] 根据上述的技术方案可知,本实施例所解决的技术问题为通过上述组成结构的信息安全管理模块,在远控智能水表终端主控制器与售水管理系统之间进行数据转发,并在转发时予以认证和加解密,从而配合自来水公司对终端的智能水表进行管理,以消除自来水公司运营中信息安全管理风险。

[0035] 而图 1 中所示出的 Oscillator 模块及其引脚 XIN、XOUT 对信息安全管理模块提供时钟信号;RAM 存储器用于存储模块运行中的临时数据;VCC 与 VSS 两引脚为信息安全管理模块提供工作电源,该电源应是持续供电而不能由远控智能水表终端主控制器的引脚提供。

[0036] 再参考图 1 所示,在本发明用于解决技术问题更加优选的一个实施例中,提供一

种上述处理器对售水管理系统身份验证及事务执行的具体方式,即在处理器接收到来自于第一数据接口的外部数据时,根据外部数据对售水管理系统进行身份认证,当认证结果判断为合法时,则对加密数据包进行解密及完整性校验,反之则复位初始状态;

[0037] 数据完整性校验通过后,对数据的有效性进行验证,反之则复位初始状态;

[0038] 当数据有效性验证通过后,对数据中包含的事务进行预处理,并通过第二数据接口从远控智能水表终端主控制器中获取相应的返回信息,将所述返回信息加密后通过第一数据接口返回给数据传输模块,当得到有效确认后则将预处理结果予以认可且储存相关的操作信息,并向远控智能水表终端主控制器发送操作指令;反之则放弃预处理结果或作缓存处理,即在预先设定的时间内没有收到数据传输模块的确认结果,例如在三分钟内未收到数据传输模块的确认信息,则复位初始状态;前述的缓存处理是指将预处理结果指令进行暂存,当处理器再次被唤醒且收到数据传输模块的确认信息时,则以同样的方式向远控智能水表终端主控制器发送操作指令。

[0039] 上述的技术方案中还包含了本实施例中外部数据从售水管理系统身份验证到外部数据中的事务被处理器所执行的整个流程,通过上述流程的程序设置,进一步加强了信息安全管理模块中对收到信息执行的安全性。而上述多次提到的处理器复位初始状态,即为复位处理器在执行上述任意一个操作之前的状态,例如处理器在接收到外部数据之前进行身份验证的状态为休眠状态,当收到外部数据由休眠状态被唤醒,但对售水管理系统的身份认证判断为非法时,处理器则恢复休眠状态,不进行任何操作,其它步骤中处理器复位的情形也基本与前述相同,当验证失败时,处理器可将操作记录予以储存。

[0040] 而同样的,在本发明的另一实施例中,为实现通过不同权限对信息安全管理模块进行管理,需在上述的 FLASH 存储器内预置协议限制条件与多个不同的密钥程序,其作用为在信息安全管理模块分别与售水管理系统中不同分级的子系统进行数据交换时,处理器根据外部数据的加密密钥与 FLASH 存储器中预置的多个密钥程序相比较,从而认证售水管理系统的身份,并在加密数据包解密及完整性校验通过后,根据协议限制条件验证数据在当前身份下的有效性,判断是否对数据中的事务进行预处理;

[0041] 参考图 2 所示,为满足目前大多远控水表的内部结构,上述第一数据接口还接入 IC 卡信息交换模块,用于在接收到来自于 IC 卡信息交换模块的外部数据时将其传输至处理器,处理器对所述外部数据执行与来自于数据传输模块的外部数据相同的校验。

[0042] 根据本发明的另一实施例,正如上述所提到的,为便于处理器预处理结果的缓存,在信息安全管理模块中还可设置相对独立的 EEPROM 存储器,并将 EEPROM 存储器也接入处理器,用于存储处理器对远控智能水表终端主控制器的相关操作信息、处理器对外部数据中事务的预处理结果,以及处理器验证的失败记录,而在 FLASH 存储器中还设置有可被处理器利用的其它程序,即处理器对远控智能水表终端主控制器的相关操作信息一旦存储至 EEPROM 存储器中后,将不可删除与修改,以便使信息安全管理模块的运行状态留下完整的记录。

[0043] 参考图 2 所示,上述实施例中的远控智能水表信息安全管理模块在实际应用中,接入远控智能水表终端主控制器与数据传输模块之间,而水表的内部结构与现有的远控智能水表无异,其主控制器分别接入阀控模块、水流测量模块、显示模块与存储器模块,主控制器根据信息安全管理模块的操作指令控制阀控模块,并将相应的水流量数值及相关信息

在显示模块中进行显示,而根据前述的原理,该远控智能水表信息安全管理模块可直接集成应用于常规的远控智能水表中,通过数据传输模块以无线或有线的形式直接从远程的售水管理系统获得相应的外部数据,从而执行上述的操作;而除此之外,还可适应性的改进应用于其它通过电子信息进行远程管理的计量装置。

[0044] 上述实施例所提到的处理器为信息安全管理模块的核心部分,用于执行相应的程序以及数据加密,在本发明的又一实施例中,上述处理器为直接采用现有技术中可执行加密算法的中央处理器或单片机,例如 EFM32 等。

[0045] 基于上述实施例所需的数据通信方式,发明人参考现有技术,选用了现有技术中部分的传输技术实现处理器与接口之间的通信,其中数据传输模块可采用网络通信模块或总线通信模块,并且与前述的数据传输模块相对应,上述实施例中用于与数据传输模块进行唯一通信的第一数据接口可采用网络通信接口或总线接口。

[0046] 更进一步的,上述网络通信接口可采用无线或有线的形式,无线网络接口可采用 RF 模块接口、Zigbee 模块接口、WiFi 模块接口、红外线模块接口及蓝牙模块接口当中的一种或多种,有线网络接口可采用光纤传输接口、数据线传输接口及电力线传输接口当中的一种或多种;上述总线接口 Mbus 总线接口、RS485 总线接口、CAN 总线接口当中一种或多种。

[0047] 而相应的,上述实施例中处理器与远控智能水表终端主控制器进行通信的第二数据接口最好与常规主控制器相匹配,例如 USART 接口、SPI 接口或 I2C 接口等串行接口,以增加信息安全管理模块集成与智能水表上的兼容性。

[0048] 再参考图 1 所示,为进一步保证信息安全管理模块中数据加密及解决的安全性,最好在其内部设置独立的加密模块,并将该独立的加密模块接入处理器,用于对信息安全管理模块与售水管理系统、远控智能水表终端主控制器数据交换的多级加解密,并辅助处理器获取售水管理系统的加密密钥进行身份认证,并参考现有技术中安全性较高的加密方式,优选采用 AES(密码学中的高级加密标准,英文 Advanced Encryption Standard 的简称)或 3DES(三重数据加密算法,英文 Triple Data Encryption Algorithm)对信息安全管理模块中往来的数据进行加解密。

[0049] 再参考图 3 所示,多个不同厂商生产的远控智能水表集成上述的信息安全管理模块后,智能水表向外的所有通信数据都通过信息安全管理模块加解密后转发,而信息安全管理模块的内部程序是唯一的,因此售水管理系统可将信息安全管理模块视为终端,用以管理智能水表,即以一个售水管理系统兼容各种品牌、类型的智能水表进行集中管理,有效降低自来水公司对区域内不同品牌、类型的智能水表整合管理的难度。如图 3 所示,远控智能水表与售水管理系统的通信路径为:表端通过上层多级通信设备,如采集器,中继器,集中器等,直接到达售水管理系统。通过上述路径,表端直接与售水管理系统实现数据传输。

[0050] 除上述以外,还需要说明的是在本说明书中所谈到的“一个实施例”、“另一个实施例”、“实施例”等,指的是结合该实施例描述的具体特征、结构或者特点包括在本申请概括性描述的至少一个实施例中。在说明书中多个地方出现同种表述不是一定指的是同一个实施例。进一步来说,结合任一实施例描述一个具体特征、结构或者特点时,所要主张的是结合其他实施例来实现这种特征、结构或者特点也落在本发明的范围内。

[0051] 尽管这里参照本发明的多个解释性实施例对本发明进行了描述,但是,应该理解,本领域技术人员可以设计出很多其他的修改和实施方式,这些修改和实施方式将落在本申

请公开的原则范围和精神之内。更具体地说,在本申请公开、附图和权利要求的范围内,可以对主题组合布局的组成部分和 / 或布局进行多种变型和改进。除了对组成部分和 / 或布局进行的变型和改进外,对于本领域技术人员来说,其他的用途也将是明显的。

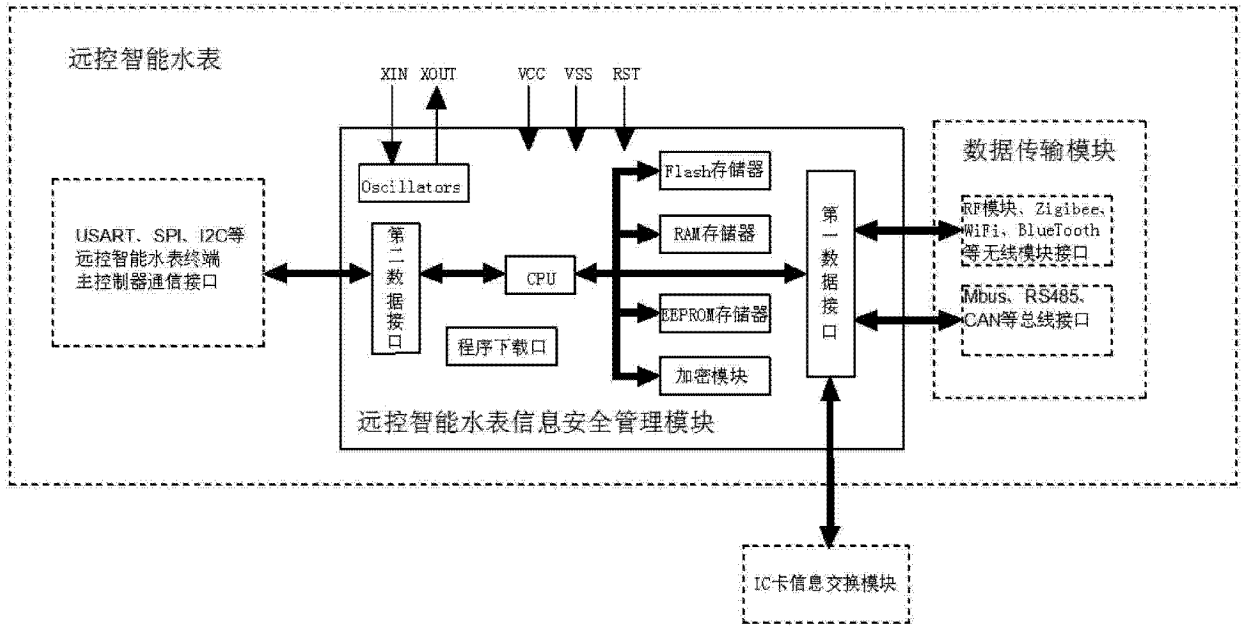


图 1

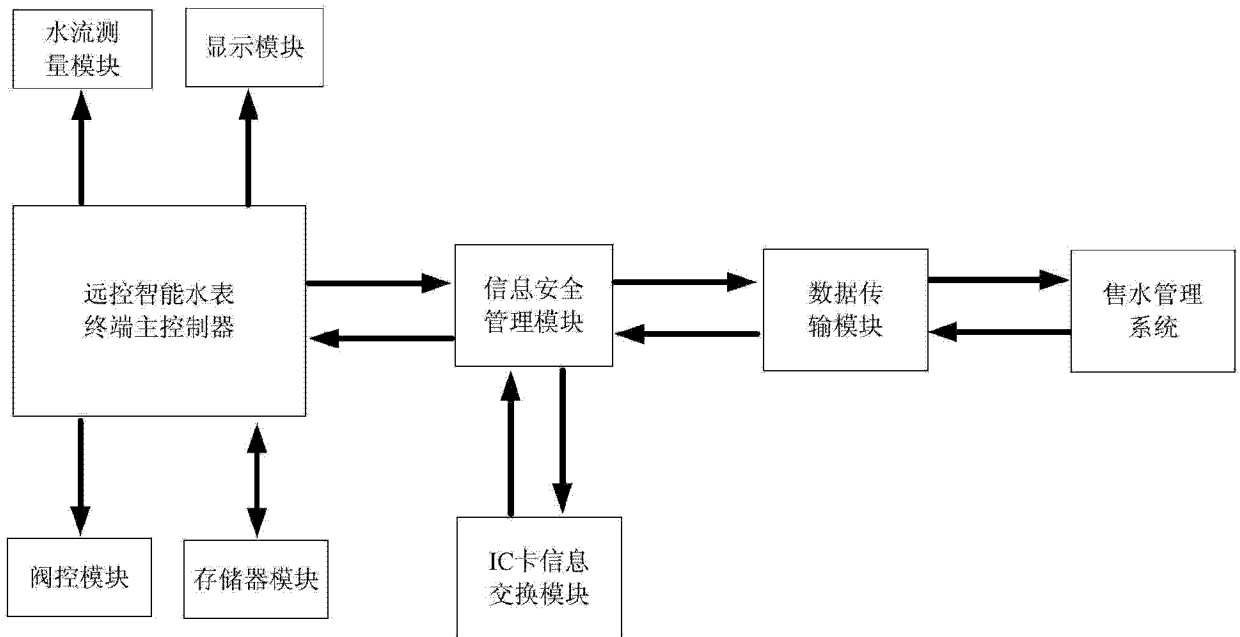


图 2

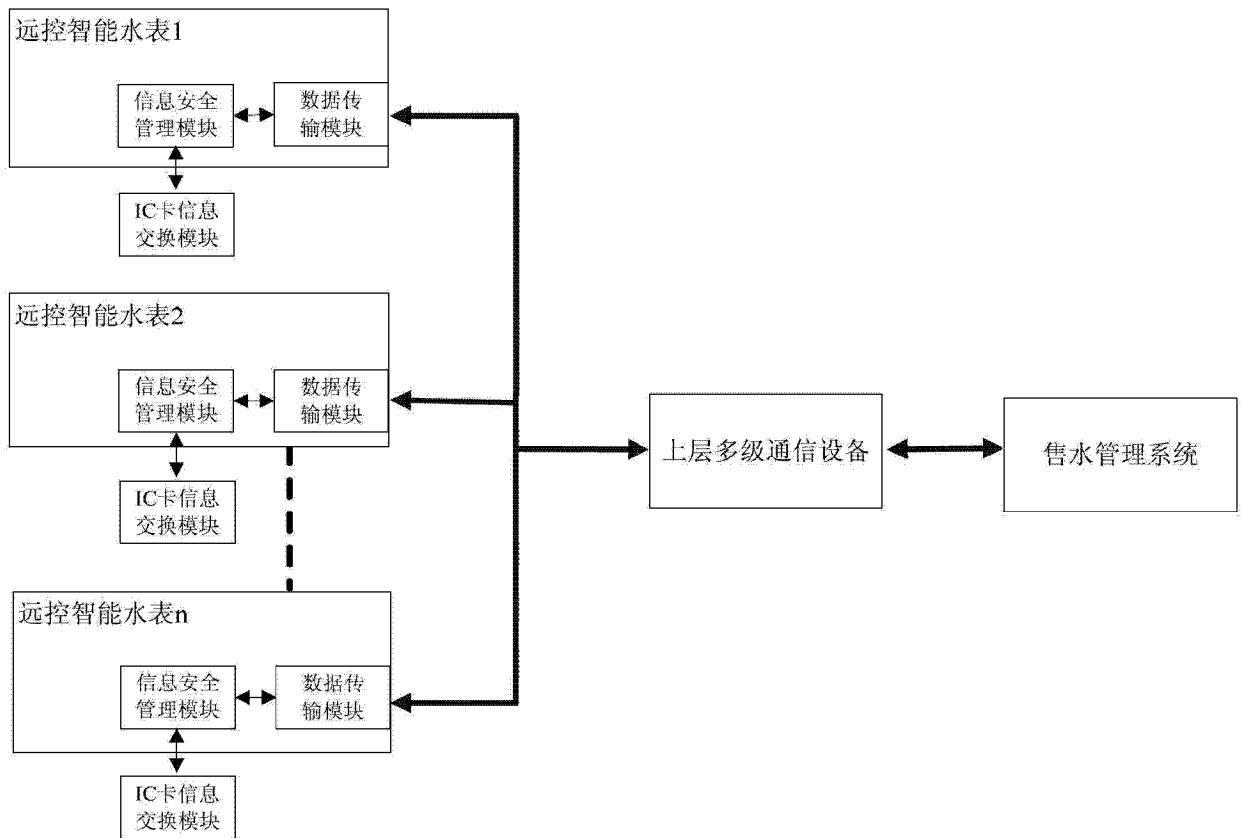


图 3