

支持远程安全管控的设备体系结构^①

赵 俭

(解放军信息工程大学, 郑州 450000)

摘 要: 针对设备远程安全管控的实际应用需求, 研究提出一款支持远程安全管控的设备体系结构, 给出设备工作流程和各模块功能结构. 该体系结构与早期设备能够有效兼容, 并具有可信特征以保证设备运行安全, 设备采用模块化设计, 各功能模块可根据应用需求进行灵活配置, 同时, 设备支持紧急情况下敏感信息的自动销毁, 能够有效提升设备安全管理水平.

关键词: 远程管控; 体系结构; 信任管理; 自动销毁; 实验验证

Architecture of the Remote Control Equipment

ZHAO Jian

(The PLA Information Engineering University, Zhengzhou 450000, China)

Abstract: Oriented at the actual application demands of the remote control with the information security equipment, this paper proposes an information security equipment structure supporting remote control, and presents the workflow and functional structure of the equipment module. The structure is compatible with the early equipment effectively, and has characteristics of credible to ensure the safe operation of the equipment. The structure adopts module design. Each functional module can be configured flexibly according to application requirements. At the same time, the equipment supports destroying the sensitive information automatically in emergency cases, which can effectively improve the level of safety management of equipment.

Key words: remote control; system structure; trust management; automatic destroy; experimental verification

随着信息技术的不断发展, 信息安全问题日益突出, 为保障各类信息系统的安全, 各种安全防护设备得到广泛应用, 然而这些安全设备自身的安全可控是其能够实施安全防护, 发挥效益的基础. 当前受部分安全设备结构设计的限制, 尚不能全面有效地实现设备的远程安全管控, 为从根本上解决这一问题需要研究设计一套新型设备体系结构, 该结构应该具有以下特性:

1) 兼容性: 保证新型体系结构的安全设备与早期设备的有效兼容, 确保设备更新换代的渐进性, 降低设备更新对正常业务开展的影响.

2) 可信性: 新型体系结构必须具有可信特征, 保证设备在运行过程中的可信可靠, 从而保证设备的运

行安全, 降低被攻击的风险.

3) 灵活性: 新型体系结构要求具有模块化结构框架, 能够对功能进行有效的裁剪, 从而根据不同应用需求进行功能配置.

4) 安全性: 新型体系结构不但要保证安全设备自身敏感信息的安全, 确保敏感信息能够在危急情况下的自动销毁, 同时还要保证监控部件的安全, 使其不成为整个系统安全的瓶颈.

远程控制在各行各业得到广泛应用, 文献[1]研究提出一种PSM电源远程控制系统的通信方法, 文献[2]设计了一款无线远程控制系统, 文献[3-8]基于网络技术研究了一系列远程控制系统, 这些远程控制系统的研究对具备远程安全管控功能的新型安全设备体系结

^① 基金项目: 国家自然科学基金(60130607)

收稿时间: 2016-04-11; 收到修改稿时间: 2016-05-12 [doi:10.15888/j.cnki.csa.005510]

构设计提供了有价值的参考。

面向远程控制功能的安全设备应该具备以往设备所没有的环境状态监测模块和可信检测单元,从而保证能够对设备的运行状态和运行环境进行有效监测,同时保证系统运行的可信可靠。面向远程控制的新型安全设备体系结构设计应遵循如下设计准则:

1) 专一准则:设备敏感资源的销毁只能由设备系统本身完成,任何其他设备都不具备该能力,确保销毁功能的专一性,从而降低资源误销毁概率,保证系统安全稳定的同时也降低系统被攻击的危险。

2) 独立准则:所有辅助远程控制的模块或单元仅仅是为安全设备提供环境及自身状态信息,提供资源消耗的参考数据,不参与敏感资源销毁过程。同时除安全设备自身外任何其他辅助单元都不能直接或间接访问敏感资源,保证其与敏感资源的物理和逻辑隔离。

3) 安全准则:所有辅助远程控制的模块或单元,必须具有完整的安全体系结构,不能成为设备的安全瓶颈,更不能由于其自身的安全性对设备造成威胁。

以上设计准则主要是为了保证设备的安全性和可用性,以期达到在设备远程控制等相关功能模块或单元增加的情况下不给设备自身带来额外安全风险,同时又能保持与设备彼此间的独立性,做到即插即用,方便集成,有则提高安全管理水平,无则维持原有安全强度,实现最大限度的提供安全保证又不增加任何额外安全风险。

1 面向远程安全管控的设备体系结构

面向远程安全管控的设备体系结构框图如图 1 所示。

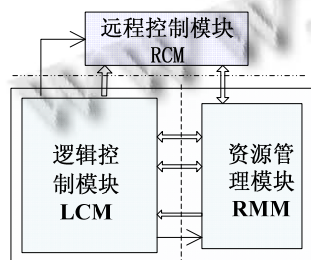


图 1 支持远程管控的设备体系结构

具有远程管控功能的设备体系结构主要包括三个部分(虚线隔开):远程控制模块(RCM, Remote Control Module), 资源管理模块(RMM, Resource Manage Module)和逻辑控制模块(LCM, Logical Control

Module), 具体如下:

1) 远程控制模块(RCM)主要完成环境信息的采集、无线数据的收发等功能。该模块通过无线传感器网络或移动通信网络接收控制端指令并完成数据的上传,可根据自身对环境信息以及周围其它设备信息的采集随时向资源管理模块提供设备安全参数。

2) 资源管理模块(RMM)能够根据 RCM 模块发送的设备状态、环境参数以及设备运行情况对设备进行安全性评估,在设备处于危险或危急状况下能够给出警报信息并实施敏感资源的销毁工作。

3) 逻辑控制模块(LCM)主要完成系统状态监测、代码完整性检查、用户接入认证等正常的业务功能,也要对系统进行可信性检测,确保系统运行的可信可靠。

该设备体系结构在不同情况下可以支持四种敏感资源销毁方式,多种销毁方式的存在能够保证资源销毁的可靠性和及时性,四种销毁方式具体如下:

1) 敏感资源在线销毁:设备在线条件下,敏感资源可以通过网络方式进行销毁,该方式方便快捷,可靠性高,可以完成批量设备敏感资源的销毁。

2) 敏感资源远程销毁:通过远程控制模块设定的相关指令,资源管理模块完成对自身的安全评估后,资源管理模块可以进行敏感资源的销毁。

3) 敏感资源自动销毁:在没有任何一种通信方式能够确认自身安全,并且自身安全评估危险的情况下,资源管理模块可以自动销毁敏感资源。

4) 敏感资源手动销毁:具备较高权限的管理员可以在通过认证的前提下进行敏感资源的手动销毁。

面向远程安全管控的新型设备体系结构设计的最大特点就是远程控制模块、敏感资源存储模块与其他功能部件进行独立设计,保证彼此间运行的独立性和互不干扰,同时系统添加了环境及状态信息采集单元,以评估设备自身的安全性。

2 面向远程安全管控的设备功能模块设计

2.1 远程控制模块结构

远程控制模块结构如图 2 所示,整个模块由传感单元、电池及充电管理单元、MCU 片上系统、GSM 模块和 ZigBee 射频模块以及用于连接远程控制接口和设备状态监测单元的两条总线构成。

其中传感单元主要用来感知环境信息、收集设备状态,并将这些信息整理后适时送入资源管理模块进

行安全评估。GSM 模块和 ZigBee 射频模块主要用来完成无线信号的收发, 其中 GSM 模块是可选的, 对于通信距离超出 ZigBee 网络覆盖范围情况下需要使用, 而 ZigBee 模块则是必选。在设备掉电的情况下, 远程控制模块可以利用电池进行供电, 设备上电时可以利用设备提供的电源线进行供电, 同时对电池进行充电。

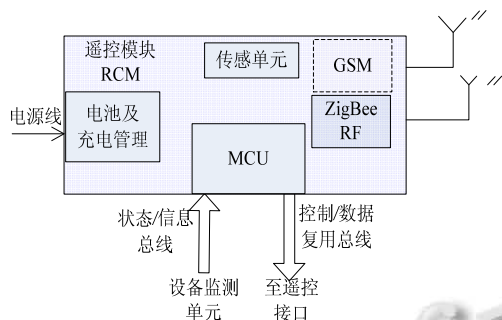


图2 远程控制模块

远程控制模块最大的特点是系统的独立性, 只完成环境监测、设备状态信息获取和无线数据收发等功能, 它只是为设备敏感资源销毁提供环境参数及相关命令, 而不参与到具体销毁操作过程当中。

2.2 资源管理模块 RMM 结构

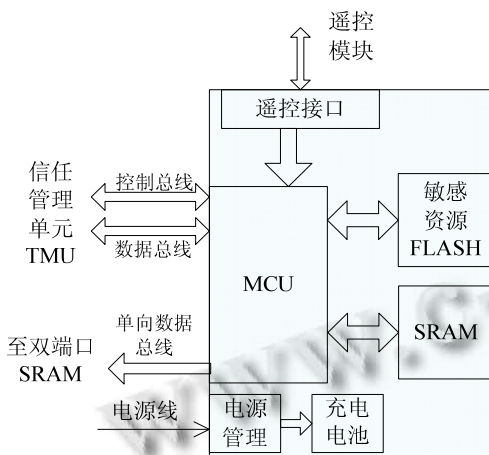


图3 资源管理模块

如图 3 所示, 资源管理模块主要由微处理器, 敏感资源 FLASH, SRAM 以及电源管理芯片、充电电池和相关数据通信接口组成。敏感资源 FLASH 内存放设备相关的敏感资源(口令、算法、参数等); 微处理器 MCU 内部可以完成加解密和散列等相关密码算法, 以便完成通信数据的验证等功能, 保证设备运行的可靠、可信和所收到信息的机密性和完整性, 同时微处

理器通过其它模块送来的环境和状态信息完成自身安全的评估, 微处理器在确定逻辑控制模块可信可靠的条件下可以将敏感资源写入逻辑控制模块的双端口 SRAM 当中, 为正常业务运行提供数据资源。而确定逻辑控制模块是否可靠的信息来自其信任管理单元 TMU, 相关的口令更新等操作也通过与信任管理单元进行相互操作来完成; 必要时刻, 微处理器则可以擦除敏感资源 FLASH 当中的敏感资源, 保证设备安全。充电电池和电源管理芯片主要为模块提供能量支持; SRAM 主要是为了微处理器的程序运行提供空间。

从上面描述中可以看出微处理器在资源管理模块中是非常重要的, 不但要完成敏感资源销毁工作, 还要进行安全评估、口令更新等工作; 这种资源管理模块与逻辑控制模块相互独立的分体设计更加容易保证系统安全, 当某一个模块存在安全隐患时, 另一模块可以通过不配合其工作来降低系统安全威胁。

2.3 逻辑控制模块 LCM 结构

逻辑控制模块如图 4 所示, 主要由八部分组成, 下文将分别对其进行介绍。

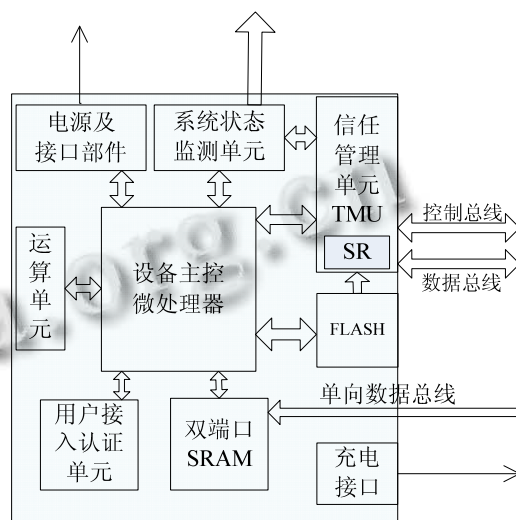


图4 逻辑控制模块

1) 设备主控微处理器: 主要负责设备的正常业务运行, 管理、执行相关指令和业务程序, 协调系统资源等。

2) 运算单元: 相当于主控处理器的协处理器, 主要完成相关算法的运行, 可以是专用的算法芯片, 也可以是可重构的芯片, 可重构算法生成的具体参数需要资源管理模块提供, 以保证算法的安全性。

3) 用户接入认证单元: 完成用户身份认证, 保证

安全设备使用的安全,同时根据用户及其权限的不同可以通过该模块向主控微处理器传达相关操作指令,完成诸如口令更新,远程控制模块选择等不同安全级别的操作,是用户与设备的接口。

4) 双端口 SRAM: 为主控微处理器提供运行空间,并在启动时,由资源管理模块载入敏感资源,以便进行相关运算操作。

5) 电源及接口部件和充电接口: 是设备的供电部件,通过充电接口可以为资源管理模块和远程控制模块提供电力支持。

6) FLASH: 是主控微处理器存放运行代码的地方,不但主控微处理器可以读取代码,信任管理单元也可以对 FLASH 中代码进行读取验证。

7) 系统状态监测单元: 主要完成系统状态的监测,比如环境温度,系统供电情况、系统运行状态、用户身份权限、设备是否被非法拆卸等,该单元主要利用一些传感器及通信信号线完成信息采集。

8) 信任管理单元 TMU: 这是逻辑控制模块上最具特色的部分,该模块完成对逻辑控制模块运行可靠、可信性的验证、采集系统状态信息,并将信息和验证结果向资源管理模块进行上报,同时在设备进行系统升级和敏感资源更新时,要通过该模块的认证后才能进行,因此可以说该模块是保证整个系统安全运行的第一关口,类似于可信计算机系统可信平台模块 TPM。信任管理单元 TMU 能够验证 FLASH 中代码的完整性,确保运行代码可靠。

2.4 信任管理单元 TMU 结构

信任管理单元 TMU 结构框图如图 5 所示,主要包括以下几个基本部件:

1) 总线控制逻辑: 主要完成数据、指令进出信任管理单元的管理工作,协调保证数据流通畅。

2) MCU 微处理器: 是信任管理单元的控制部件,协调其它各部件的工作,完成相关的数据处理等工作。

3) 状态寄存器 SR: 主要用来存放设备状态信息,环境信息,FLASH 内部代码校验信息、系统初始化口令等,该状态寄存器中的数据只能提供给资源管理模块 RMM,其他任何设备没有权限读取。

4) 随机数生成器: 用于密码运算或身份认证过程中的随机数生成。

5) 加解密引擎: 用来完成数据的加解密操作,具体加解密算法可根据实际需要选取。

6) 杂凑引擎: 主要执行一些哈希算法,完成数据完整性校验,确保数据不被修改。

7) 外部相关总线: 主要是与主控微处理器,资源管理模块和系统状态监测单元相通信的数据控制总线。

8) 信任管理单元: 主要完成系统状态,环境信息的采集以及保证系统运行可靠可信性的验证,资源管理模块根据信任管理单元的相关数据完成自身安全的评估。

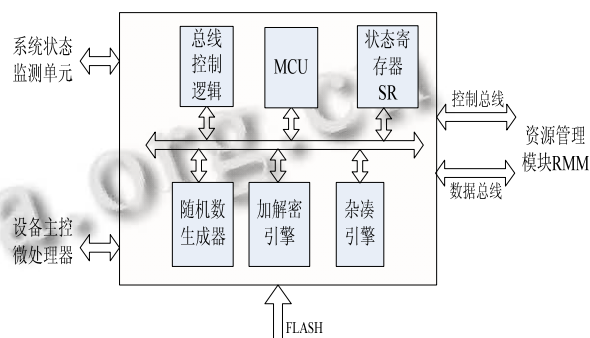


图 5 信任管理单元 TMU 结构框图

3 面向远程安全管控的设备工作流程设计

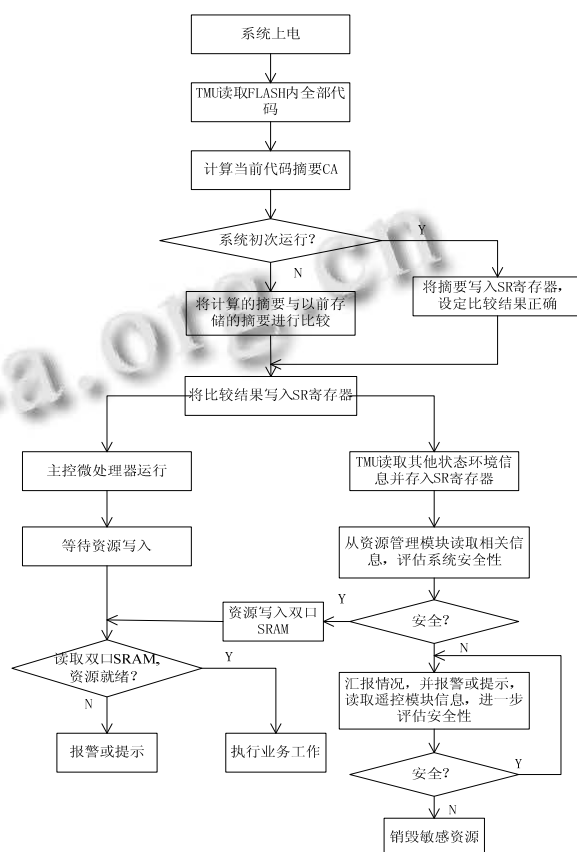


图 6 设备工作流程

面向远程安全管控的设备运行流程如图 6 所示,

设备在使用之前,必需具备以下条件:

1) 设备管理单位必须在信任管理单元 TMU 中的状态寄存器 SR 内写入以下信息: 加解密算法的初始口令 TIK (TMU Initial Key) 用于管理中心同设备间的通信加密; 各类用户的 ID, 用于评价用户权限。

2) 资源管理模块内已设定好各安全参数的阈值, 用于判断平台安全性。

从流程图中可以看出, 设备工作过程中需要对当前的状态及安全性进行评估, 在不够安全的情况下会向用户提出报警信息, 由用户来解决相关问题, 在危急的情况下会自行销毁密码资源。

4 系统实验

为验证该支持远程安全管控的设备体系结构功能, 构建如图 7 所示的系统。

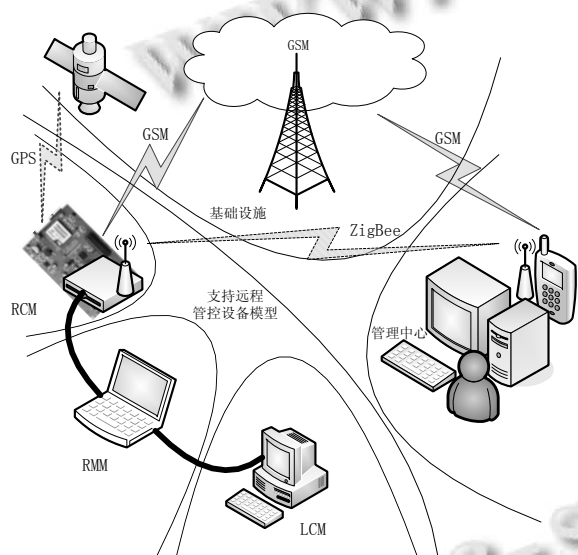


图 7 实验验证系统

该验证系统由支持远程管控的设备模型、基础设施和管理中心三部分构成。其中基础设施主要借助现有的移动通信网(GSM)和近距离个域网(ZigBee 网络)构建安全设备管控网络; 管理中心配备相应的通信模块以实现对设备的安全管理和远程控制; 支持远程管控的设备模型依据其体系结构设计, 由远程控制模块(RCM)、资源管理模块(RMM)和逻辑控制模块(LCM)共同构成, 实验验证中远程控制模块基于 TC35i 移动通信和 CC2530 的 ZigBee 通信模块以及和芯星通 UM220 定位模块等构建, 而资源管理模块和逻辑控制模块分别利用联想的 T430 笔记本和 M6900 台式机构

建, 资源管理模块(T430)和远程控制模块以及逻辑控制模块(M6900)之间直接通过 RS232 串行接口线缆连接(T430 没有 RS232 接口, 通过 USB 转 RS232 模块实现)。

依据设备工作流程, M6900 上运行模拟软件执行系统上电后信任管理单元的 FLASH 代码读取、摘要计算、结果匹配及状态记录等工作, T430 上运行模拟软件执行 GSM/ZigBee 模块数据传输、GPS 位置信息获取、FLASH 敏感资源的删除等工作。

验证时管理中心通过 GSM/ZigBee 构建的安全管控网络向受管控的设备发起删除敏感资源的管控指令, 该指令通过远程控制模块接收解析后传输到资源管理模块, 即对其中的敏感资源信息实施删除操作; 管理中心发出获取受管控设备的位置信息命令, 远程控制模块接收解析后, 由 T430 中的环境状态信息获取模块读取 GPS 模块提供的位置信息并经管控网络返回到管理中心; 其它资源管理模块和逻辑控制模块的功能验证通过编写相应的软件实现。

经实验验证, 该远程安全管控的设备体系结构具有良好的适应性, 能够满足设备远程安全管控的现实需求。

5 结语

支持远程安全管控的新型安全设备体系结构划分为功能基本独立的三个模块, 各模块之间保持有限的通信, 因此具有如下优点:

1) 数据传输单向性: 远程控制模块(RCM)与敏感资源保持逻辑上和物理上隔离, 且只能根据设备的需要为资源管理模块提供安全参数和环境数据, 无法实现对资源管理模块(RMM)的控制, 在确保数据传输单向性的同时也提高了敏感资源的安全性。

2) 资源获取认证性: 资源管理模块(RMM)在向逻辑控制模块(LCM)提供敏感资源之前, 要对逻辑控制模块(LCM)的工作状态进行安全认证, 在确保逻辑控制模块(LCM)状态和运行都正常的情况下才主动送出相关资源, 进一步保证了资源的可靠使用。同时由于数据接口设计采用单向性设计, 也使得敏感资源的传输具有单向性。

3) 系统结构灵活性: 远程控制模块(RDM)与安全设备接口设计简单, 能够实现模块的热插拔功能, 以便于系统集成和功能上的裁剪。同时远程控制模块

(RCM)的工作状态可以通过已认证用户进行灵活设置,保证模块使用的灵活性.

4) 资源销毁可靠性: 资源管理模块(RMM)除了具有普通电源接口外, 自身还备有充电电池, 能为资源管理模块长时间续航提供保障. 因此即便在设备掉电的情况下仍然可以实现在紧急情况下敏感资源的销毁.

5) 运行环境可信性: 逻辑控制模块(LCM)具有可信的特点, 从系统的启动到正常运行, 每一个环节都有信任管理单元对其进行可信评估, 并将评估结果送给资源管理模块(RMM)进行检查, 一旦发现系统配置出现问题, 则及时提出报警, 保证系统的内部程序、硬件环境的可信可靠.

参考文献

- 1 张猛,姚列英,王英翘.基于 CAN 总线技术的 PSM 电源远程控制通信系统.核聚变与等离子体物理,2015,35(1):24-29.
- 2 陈波,高秀娥,隋广洲.无线远程控制系统研究与实现.仪器仪表学报,2006,27(z1):573-574.
- 3 王义乐,宋书中,朱锦洪,代乐宜.基于网络的远程监控研究.电源技术,2013,37(12):2265-2268.
- 4 熊瑞平,殷国富.网络制造环境下的远程控制系统研究.计算机集成制造系统,2006,12(11):1848-1852.
- 5 唐洋,谢冲.井控装置无线远程控制及监控系统设计.制造业自动化,2013,35(18):51-54.
- 6 王德文,朱永利,邸剑,翟学明.基于 IEC 61850 的电力设备远程控制方法.电力系统自动化,2009,33(5):50-54.
- 7 郑娟毅.基于 ZigBee 技术的家庭 WSN 及远程控制研究.电视技术,2010,34(4):67-69.
- 8 Li J, Cao S, Duan JX, Gao PC, Hou Y. A novel remote monitoring and control system based on GSM for home security. International Journal of Online Engineering, 2015, 11(4): 34-40.