

安全隔离网闸在油田物联网中的应用探讨

张艳

(北京和利时工业软件有限公司 北京 100176)

摘要: 油田物联网系统运行的过程中,面临着信息安全风险,为确保油田物联网数据的安全性,需要通过有效的技术手段实现内外网的有效隔离,安全隔离网闸便能够满足这一需求。因此,本文主要研究安全隔离网闸的应用原理和特性,结合安全隔离网闸在我国某油田物联网中的实际应用,探讨安全隔离网闸的实际应用效果,以保证油田物联网信息的安全性。

关键词: 安全隔离网闸; 油田; 物联网; 应用

0 引言

安全隔离网闸也就是安全隔离和信息交换系统,最早用于网络隔离的工具,为物理隔离卡,主要应用于两个隔离网络之间,通过模拟人工的方式实现信息交换。第一代安全隔离网闸主要采用单刀双掷开关,对内外网处理单元的共享存储设备分时存取来实现数据交换,能够在空气缝隙“AirGap”隔离的情况下实现数据交换。第二代安全隔离网闸则在第一代基础上创造性地采用了PET技术,使数据交换时能依靠私有通信协议、专用硬件通信卡以及加密签名来完成,这种方法不仅可以保证数据的安全性,还能够实现内外网间的数据快速交换,同时还支持多网络应用。油田物联网系统运行过程中容易出现信息安全问题,将安全隔离网闸有效应用于油田物联网中,对于信息安全防护具有重要的意义。

1 安全隔离网闸的应用原理及特性分析

1.1 应用原理

安全隔离网闸在正常条件下,其内外网之间处于完全断开状态,当外网存在向内网传输数据需求的情况下,外部服务器便会马上向隔离设备发起非TCP/IP协议属性的数据连接,使隔离设备能够将全部协议进行隔离,同时还会针对数据展开病毒扫描以及数据分析,将已完成检测的、安全的原始数据向存储介质之中写入。数据写入完成之后,隔离设备便中断与外网之间的连接,然后向内网非TCP/IP协议发送数据连接请求,所有的数据向内网推进,同时交由应用系统处理。当控制中心获取交换信号之后,隔离设备切断同内网之间的连接。当数据传递由内网向外网传递的情况下,其原理也是如此。

1.2 特性

安全隔离网闸在实际应用中具有如下特性:

(1) 从硬件架构角度来讲,安全隔离网闸主要是隔离硬件与双主机联合构成,所以系统的安全性表现比较突出;

(2) 安全隔离网闸主要应用层工作,具有文件同步、数据库以及定制开发等多种功能,在对网络进行隔离的过程中,会在数据层将网络连接断开,将全部TCP/IP协议的网络通信断开,能够对TCP/IP协议环境下出现的木马

病毒进行有效的阻隔,有效保障信息安全;

(3) 安全隔离网闸处于主机模式的情况下,全部数据均需进行落地转换,此时内部网络信息将被完全屏蔽;

(4) 安全隔离网闸无法进行内网与外网对话,连接在内网及外网的主机终止;

(5) 安全隔离网闸在工业生产领域的网络控制方面比较常用,在公用通信、办公网络等方面的安全防护均可发挥突出效果;

(6) 网闸主要采用了总线技术、SCSI技术以及光纤传输技术等,可做到单向或者是双向网络隔离。

2 应用案例分析

为了进一步探讨安全隔离网闸在油田物联网系统中的实际应用,本文将以国内某油田为例,对安全隔离网闸在该油田物联网系统中的具体应用展开探讨。

2.1 油田物联网建设概况

该油田物联网建设主要是依据集团公司制定的网络信息化建设要求进行。在对隔离网闸进行选择方面,该油田公司采用了传统网闸,在硬件结构方面,采用了隔离硬件与双主机模式,同时使用了流处理芯片以及专有隔离芯片,在进行网络通信时,主要通过内部四友协议来实现数据安全传输,通过网闸对通用网络协议进行阻断。该网闸工作园林与二极管单向导电颇为相似。为了便于日常业务访问,该网闸以安全监测结果为依据,通过内外网解析应用协议,在一端对该协议进行隔离,并获得数据,另一端又将应用协议恢复。该解析囊括了所有常见的应用协议,同时能够通过数据库访问,该网闸的安全是通过安全监测来实现的,容易造成缓冲区溢出、木马病毒入侵以及SQL注入,通过解析协议之后,应用便能够通过该隔离网闸,造成攻击的载体形成。所以,在应用协议的条件对网闸解析事实上属于安全网关,具备数据交换功能,但并不具备网络隔离作用,所以为了保证该油田物联网系统的信息安全,必须采用一种安全的隔离网闸,传统隔离网闸的工作原理见图1所示。

2.2 安全隔离网闸在油田物联网中的设计

从上述物联网系统的建设概况来看,虽然已采用了隔离网闸,且能够实现数据传输,但在保证数据信息安全性

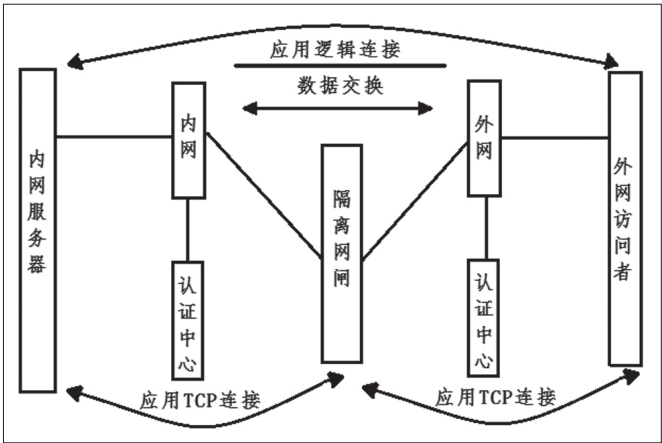


图 1 传统隔离网闸工作原理图

方面仍有不足，所以为了确保该公司物联网运行的安全性，需要对该公司现用的隔离网闸进一步优化，使之不仅能够发挥数据交换的作用，而且还能够对物联网系统的安全性予以保障。这需要在满足该油田物联网网闸设计目标，即确保通讯隔离的条件下实现数据交换，重点是保证安全性，所以隔离网闸设计既要隔离和交换控制逻辑进行有效设计，又要实现业务数据的自动转换（设计原理见图 2）。

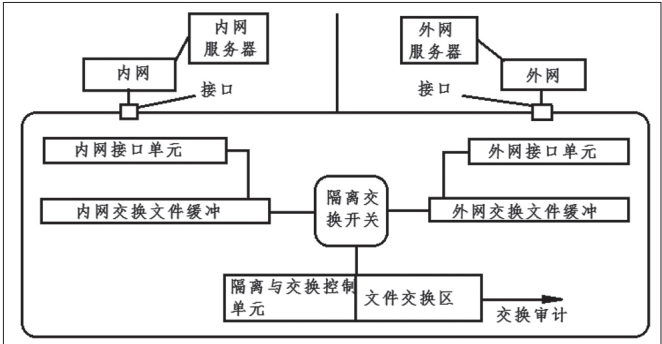


图 2 安全隔离网闸设计的原理图

2.3 安全隔离网闸在油田物联网系统中的应用

根据上述设计目标及设计内容，可以通过压力测试、市场调研等方式对安全隔离网闸进行合理选择，最终该公司选择了高端的单向网闸。该网闸主要采用信息交换与安全隔离系统架构。该系统包括内网及外网主机系统以及隔离交换矩阵，两个系统分别同内网及外网相连，主要进行协议分析以及信息获取。隔离交换矩阵是以安全策略为依据对信息的安全性进行检测，并负责内网与外网之间的信息安全交换，从而使该系统能够形成多网络隔离系统，并且能够通过专用的硬件将各方信息进行传输。同时，被隔离的内外网之间并不会产生任何物理连接，内网系统与外网系统之间并不存在网络协议相关的逻辑连接，隔离交换的数据均属于应用层数据，数据交换呈现出突出的私有属性，无法对其进行编程，在一定程度上保证了数据信息的安全性。

通过应用该安全隔离网闸，使该油田物联网中多个数据库实现了单向同步，并将各安全域间信息交换方面存在

的问题得到有效解决，同时，还能够实现对应用层信息的实时检查，访问并控制信息交换底层，从而保障油田物联网运行的安全性及可靠性。

2.4 安全隔离网闸应用的注意事项

虽然安全隔离网闸能够同时实现信息交换和安全隔离，使油田互联网系统运行的安全性得到提升，但是安全保障与油田生产视频子网之间并不能够实现平台之间的互动，所以在对办公网与视频网进行隔离的过程中，应该使用视频网闸。该网闸工作的主要原理在于油田物联网子系统能够通过协议检查协议内容及格式，并对协议内容进行分析，从而对控制信令与视频数据进行有效区分，仅允许视频数据进行单向传输，允许控制信令进行双向传输，并对数据来源进行全面检查，对非法数据的输出及输入进行阻止，同时针对输出的信息实施“白名单”检查，以免造成一些非授权的重要信息外泄，引发信息安全风险事件。

3 结语

安全隔离网闸对于油田互联网系统运行的信息安全发挥着至关重要的作用，作为油田互联网运管人员不仅应该具备安全意识，还要充分意识到网闸业务协议解析在信息安全方面带来的新问题、新挑战。对于网闸而言，并非功能越多越好，而是应该从网闸所处网络位置及作用目标出发，实现网闸的使用目的。在本研究中，将我国某油田物联网系统作为研究对象，从该油田物联网系统运行需求来看，既需要安全的信息交换，又需要实现安全隔离，其作用便在于实现安全服务，而网闸开通服务的数量和种类越少，物联网系统被攻击的概率便会越低；网闸交换数据的数量和类型越少，则系统承受的攻击便会越小。所以，可将网闸安全性原则表述为：在单向服务中，只是将数据交换完成，可将其他服务全部关闭；应该实施定向交换，在开展数据交换过程中，应该将操作人员指定；网闸对应用协议的解析不予支持，不将业务应用透传，仅作为文件数据传输使用，对 FTP、HTTP 等多协议不支持通过，对数据库访问也不支持通过；网闸仅作为数据传输，不作为应用互联，通过终止应用协议，从而使油田物联网受到的攻击和入侵丧失传播载体，从而确保油田物联网运行的安全性。

参考文献：

[1] 张炳铖,刘冠辰.物联网技术在数字油田中的应用探析[J].信息周刊,2020(3):1-1.
[2] 任丽杰.物联网信息技术在油田地面数字化建设中的应用[J].信息系统工程,2020(7):20-21.
[3] 石国伟.浅析物联网,大数据及云计算技术在油田生产中的应用[J].中国管理信息化,2020,23(8):97-98.
[4] 赵春生.物联网技术在油田中的应用[J].信息周刊,2020(4):1-1.
[5] 王宏宇.物联网应用技术在数字化油田建设中的应用分析[J].石河子科技,2020(6):2.

作者简介:张艳(1983.11-),女,汉族,山东临沂人,硕士,研究方向:计算机应用技术。