一种基于照相数据传送原理的工业网络隔离技术和产品

★王建 北京优化佳控制技术有限公司

摘要：本文介绍了一种基于照相数据传送原理的工业网络隔离技术，由于采用了非网络化的数据传送系统，可以对现有和未来基于网络的病毒和黑客攻击进行有效阻断和隔离。经过近十年的研究开发已经形成了多个系列数十种产品，并在大规模的工业网络中长期应用，工作稳定可靠。在最近的WannaCry病毒攻击事件中，该技术成功地阻断了攻击，使隔离保护区内的DCS和生产装置安然无恙。

关键词：工业网络安全；网络隔离；照相数据传送；WannaCry病毒；DCS安全；数据库；数据采集网络

1 概述

目前，在工业生产过程中，广泛采用计算机（DCS，分布式控制系统）控制生产过程。而在绝大部分工厂里，这些DCS系统又与厂内的实时数据库、办公网络相连，如图1所示。在与DCS相连的网络上有成百上千台计算机。如果其中的某一台计算机感染病毒，就有可能通过计算机网络传导到DCS中。

如何防止病毒和黑客通过数据采集网络攻击工业控制计算机系统，是一个典型的边界防护问题。在传统的方法中，一般是采用防病毒软件、工业网关、网闸等来实现。但目前的网络攻击技术，有些已经可以成功越 过这些防护措施对控制系统进行攻击。

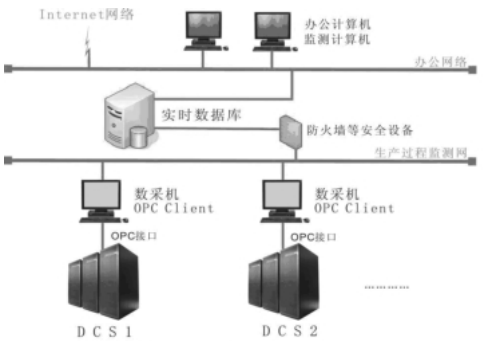

图1 常规数据采集系统

对这种常规的数据采集系统，存在着以下几方面的网络安全问题：

（1）这种数采监测系统的一个明显问题是过程控制计算机与局域网络存在物理连接；

（2）这种数采监测系统使得过程控制计算机可能会受到来自办公管理网上的病毒感染或黑客的攻击；

（3）尽管有软硬件的防病毒软件和防火墙，但并不能保证过程控制计算机的绝对安全，也会造成不可预测的后果。

2 照相数据传输原理

DCS之所以会感染病毒，实质是DCS与实时数据库和办公系统存在物理的网络连接，用于传送生产装置的数据。如果把这个网络切断，DCS就不会通过网络感染病毒。但是这样一来，实时数据库便无法

获得生产数据。能不能有一种方法，不用计算机网络把DCS的生产数据传送到实时数据库呢？如果能够实现，就彻底断绝了计算机病毒和黑客的传播通路，从本质上保证了DCS的安全。

北京优化佳控制技术有限公司（以下简称优化佳公司）经过了十余年的研发，投入大量人力物力，最终发明了一种“照相数据传送技术”，可以在无网络情况下把DCS数据向实时数据库传送，并且实现了技术的商品化。该技术2009年获得中华人民共和国发明专利（专利号：ZL200610064971.8），并由于该技术的新颖性，正在国际上四十余个国家申请专利，其中有些已获得专利证书，如表1所示。

2015年该技术还获得工信部中国电子信息产业发展研究院颁发的“2015年度中国工业控制网络安全最佳解决方案奖”和“2015年度中国工业控制网络安全创新企 业奖”。

表1 照相数据传送技术所获国内外的各种专利

	专利号
中华人民共和国	ZL 2006 1 0064971.8
中华人民共和国	ZL 2007 8 0018261.4
美国	US 8,341,741 B2
加拿大	2,645,722
欧洲	2003815
俄罗斯	2426248
韩国	10-1146184
日本	4971420

2.1 照相数据传送的原理

不通过网络又如何传送数据呢？图2、图3显示了照相数据传送的基本原理。

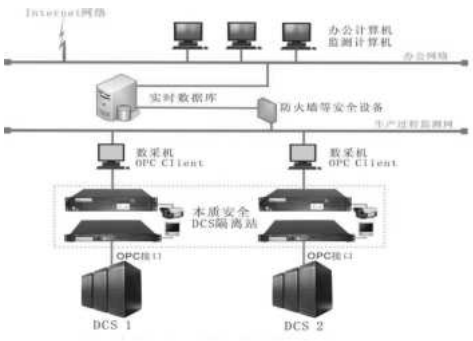

图2 本质安全DCS隔离站网络结构图

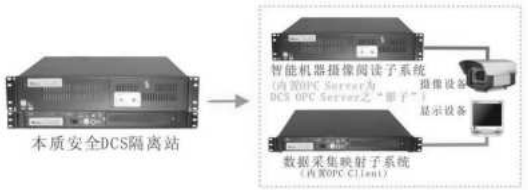

图3 本质安全DCS隔离站网络结构图

从图2、3中可以看出，DCS要上传的数据由专门的数据采集计算机采集，并且将这些数据显示在计算机的屏幕上。另外有一个摄像系统将屏幕上显示的实时数据定时自动拍摄下来，拍下来的数据画面经过智能机器阅读系统的自动解读后得到要上传的数据，通过局域网送到实数据库和办公网上。这样，局域网和DCS之间完全没有网络的物理连接，病毒和黑客就不可能通过网络传到DCS中。无论病毒如何变化，都可以从本质上保证DCS的安全。

目前，优化佳公司应用该原理，将数据采集计算机，显示、摄像系统和智能机器阅读系统集成在一起，研发成商品化的本质安全DCS隔离站。该站已经在多个DCS系统中长期稳定运行，如图4所示。

图4 本质安全DCS隔离站组实物

3 基于照相数据传送技术的系列产品

基于照相数据传送专利技术，优化佳公司开发出一系列的商用产品，产品总览如图5所示。图中显示了各具体产品和在网络中使用的位置。

3.1 本质安全DCS隔离站系列产品

（1）PDT单输入本质安全DCS隔离站

该产品提供一个输入接口和一个输出接口。其中输入接口可与DCS端的一个OPC Server连接，采取上

传数据。这些数据经过照相数据传送后，进入隔离站内置的OPC Server，外部的OPC Client 通过隔离站输出接口连接到内置OPC Server 取数。

（2）PDT多输入本质安全DCS隔离站

该产品提供多个输入接口和多个输出接口，每个输入接口可与相应DCS的OPC Server连接。这样，一套多输入的隔离站可以连接到多个DCS OPC Server采集上传数据。经过照相数据单向传送后，进入隔离站内置的多个OPC Server，通过多个输入接口以OPC方式输出。

（3）PDT单输入文件传输型本质安全DCS隔离站

该产品具有一个输入端和一个输出端。其中输入端可以送入要传送的文件，采用照相方式将文件单向传送后，通过输出端推出文件。该隔离站不仅可以用于DCS端向外单向传送文件，也可以用于任何需要进行文件单向推送的场合。

（4）PDT多输入文件传送型本质安全DCS隔离站

该产品具有多个输入端和一个/多个输出端。每个输入端可以送入各自的要传送的文件，采用照相单向传送后，通过一个或多个输出端口送出。该隔离站不仅可以用于DCS端向外单向传送文件，也可以用于任何需要进行文件单向推送的场合。

（5）隔离站组故障侦测报警和自动冗余切换系统

该系统可以自动侦测各DCS隔离站的工作状态，健康状况，如发现问题，自动进行声光报警，并向指定手机发送短消息，自动冗余切换系统会向手/自动冗余控制器发出指令，把发生故障的DCS隔离站切除并将隔离系统切换到预设的备用方案上。

（6）手/自动冗余控制器

该手/自控制器接受隔离站组故障侦测报警和自动冗余切换系统的指令，将常在线的主站切换到备用站，或者从备用站切换到主站上，也可以人工强制手动进行主/备切换。除此之外，还可以实现隔离方案的手/自动切换。

（7）单输入双机手/自动冗余系统

该系统由一台常在线主隔离站和一台备用隔离站以及冗余控制器构成。当主机发生故障时，冗余控制器可以自动切换到备用机上，如果主机恢复正常工作状态，则会自动从备站切回主站。主备站也可通过手动强制切换。

（8）多备一手/自动冗余系统

该系统由多台主隔离站和一台备用隔离站构成。多台主站合用一台隔离备站。当其中某一主站发生故障时，会自动切换到备用站上。由于多台主站合用一台备站，既大大提高了隔离系统的可靠性，又大大降低了冗余成本。

（9）隔离站日志服务器

可以对隔离站组上的每个隔离站的行为进行日志记录及安全审计。

（10）隔离站运行状态远程监测系统. 该系统利用无线数据传送组件进行远程信息传送，将分散在全国各地各分部的隔离站运行状态进行集中显示监测，特别适用于大型、分散各地的工业网络隔离管理。

（11）PDT无线传送型本质安全DCS隔离站

该站在采集到上传数据之后，通过照相方法将数据进行单向隔离传送，然后这些数据通过手机移动网络传

送到远方的无线实时监测系统。该站配有本地智能诊断和修复系统，具有很高的可靠性，实现无人值守。

（12）无线远程实时监测系统

该系统有内置的实时数据库，接受无线传送系统本质安全DCS隔离站的DCS实时数据，并对分散于各地的多个远程站进行健康状态监测，数据管理和分析。

4 应用情况

本质安全DCS隔离站自2007年以来，已经在许多大型企业中应用，现在有一百多套正在现场运行，时间最长的已经运行了10年之久，历经了长期运行的考验。下面以中石化两个大型工业企业为例，介绍在企业应用的情况。

4.1 中石化某公司全厂DCS安全隔离系统

中石化某公司为年加工能力1000万吨的大型炼油企业，有19套老装置和新建大炼油1套联合装置等，经过方案设计的优化，只需采用十套本质安全DCS隔离站就可以对全厂生产过程控制网络进行彻底的网络安全防护，如图6所示。

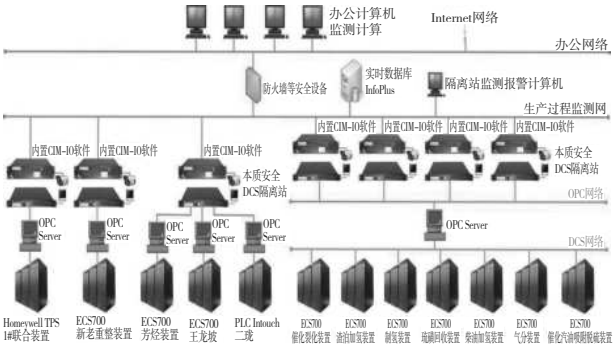

图6 中石化某公司全厂本质安全DCS隔离站配置结构图（部分）

（1）新建大炼油相关装置约20000个TAG，本质安全DCS隔离站的单站最大处理能力是6000个TAG，考虑未来新增位号的可能性，为其提供5套隔离站便可满足需求。

（2）19套老装置共计约24000个Tag ，考虑一些装置位号个数仅为几十个或几百个，从可行性，安全性、经济性多个角度进行综合分析，为其提供4套多输入，2套单输入本质安全DCS隔离站便可满足实际需求。

（3）全厂新老装置共约44000个Tag。共需10套本质安全DCS隔离站完成隔离。工程分两期进行，一期工程7个隔离站，二期工程3个隔离站。

（4）配有DCS隔离站监测系统，可以实时监测隔离站的各种工作情况及健康状况。

DCS安全隔离系统自2012年8月投运以来，运行情况良好，稳定运行至今，各应用部门对该系统都给予了充分肯定：

（1）各实时数据库安全隔离系统运行正常；

（2）采集隔离的数据完整、准确；

（3）配有专门设计的DCS隔离站监测系统。用户可查看各个隔离站所属系统运行的健康情况，记录隔离站发生的各种事件，还可以通过短信发布所发生的重要事件；

（4）系统响应快速，系统恢复用时短，系统应用影响小。

该系统于2013年10月通过中石化测试验收。

4.2 某化工厂本质安全隔离站应用情况

某化工厂本质安全DCS隔离项目于2015年1月签订合同，2015年9月投入运行。

在该项目中，采用北京优化佳公司的照相数据传送专利技术，使用8套PDT4000本质安全DCS隔离站，对合成氨装置、制氧乙炔、动力、VAE新老装置、东西循、PVA、发电124#和软水8套关键装置进行隔离，使用隔离站后，这些装置的DCS数据只能单向传送到全厂实时数据库，而外网的病毒和黑客等无法通过数据采集网络系统对DCS发动攻击，从而确保生产的安全。

该厂本质安全DCS隔离系统项目创新点如下：

（1）项目中使用了最新的PDT4000系列产品。

PDT4000系列产品是本质安全DCS隔离站第四代产品，与第三代产品相比，有着以下的技术进步：

· 可以进行位号的在线追加、编辑。以前的产品在对上传的位号进行添加或删除时，需要将隔离站离

线一段时间，这会造成数据传输的中断。现在可以在不中断数据传送的情况下进行上传数据位号的修改；

- 体积减小了1/3；
- 能耗减小了2/3；
- 硬件重新设计研发，具有更高的可靠性。

（2）采用多备一全自动冗余的新技术，大大提高系统可靠性。

在本项目中，使用了创新的8备1自动冗余方案，只要系统侦测到其中的一套隔离站有问题，会自动将隔离任务切换到备站。不仅如此，如果此后还有其他主站出现问题，只要有故障的主隔离站的传输点数不超过备站的最大能力，均会将隔离传输的任务自动切换到备站。也就是说，即便是多个主站同时出现问题，也可以同时切换到备用站。

由此可见，多备一系统技术的应用，可以在增加少量备用冗余投资的情况下，实现多套系统的全自动冗余，大大提高了系统的可靠性，使生产数据的传输得到了保证。

5 本质安全DCS隔离站成功阻断WannaCry病毒事例

2017年5月爆发的WannaCry病毒感染了某工业企业油库生产监控平台，病毒沿着数据库的数据采集网络向DCS和生产设备传播。由于事先在数据库的数据采集通道上安装了本质安全DCS隔离站，及时发挥了保护作用，阻断了病毒向DCS系统的扩散，保护了工控系统，确保生产的正常进行。

图7是该油库生产监控平台的拓扑图。

图7中，连接数采缓存机（3号机）和工控网交换机的设备是本质安全型DCS隔离站，它包含两台设备：数据采集与映射子系统（1号机）和自动摄像与智能阅读子系统（2号机），其中2号机与3号机相连，1号机和工控网交换机相连。隔离设备的任务是：保护下面的DCS系统不受上面网络中病毒和黑客的攻击，同时完成DCS系统生产数据向上面数据库的

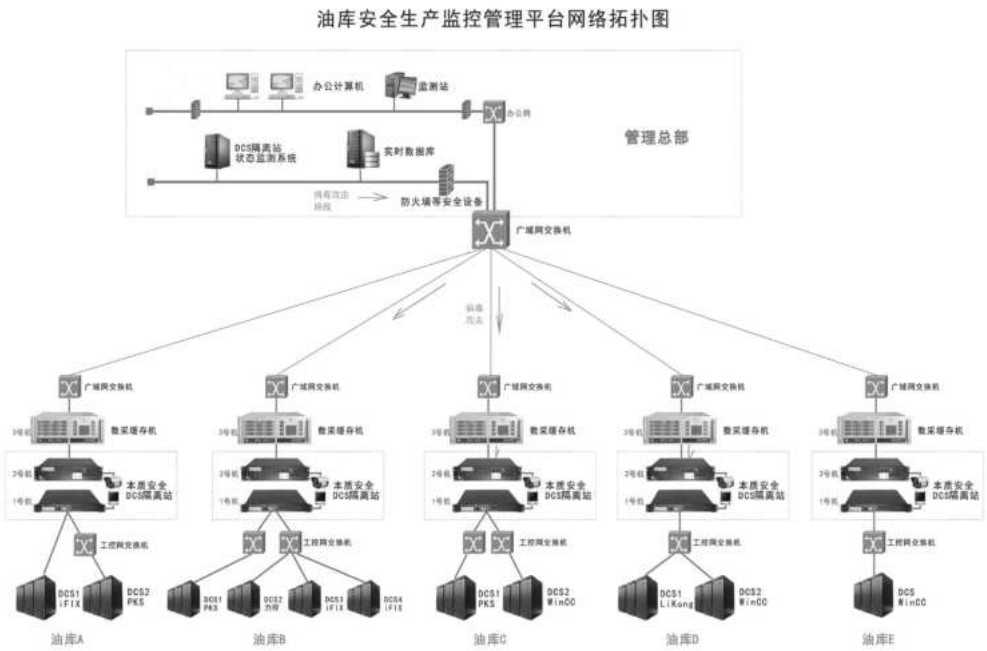

图7 某企业油库生产监控平台的拓扑图

实时传递。

在WannaCry蠕虫病毒爆发后，该监控平台受到病毒的攻击，其过程如下：

（1）病毒使管理总部的实时数据库服务器中毒。

（2）病毒通过专网扩散到各地油库，通过交换机下传到数据采集计算机，造成B、C、D三地油库数采缓存机（3号机）中毒。

（3）上述三地的病毒通过网络继续向下入侵，到达本质安全型DCS隔离站，并造成C、D两地的隔离站2号机中毒。

（4）由于本质安全型DCS隔离站具有的照相数据单向传输特性，使得2号机上的病毒无法继续扩散到1号机，阻断了病毒的向下传播，从而实现了对下面DCS系统的保护。

由此可见，在此次病毒攻击事件中，攻击被本质安全DCS隔离站阻断，确保了保护区内的工业生产设备的安全。

6 结语

基于照相数据传送技术的本质安全DCS隔离站具有如下特点：

（1）完全单向的数据传送，零比特返回,切断外部攻击通道，可以防范现有和未来的基于网络的病毒和黑客的攻击；

（2）数据正向传输采用非网络方式，无网络传输通道，可以防止DCS内网的间谍软件和病毒黑客利用网络通道向外传输情 报，向数据库端发起攻击；

（3）具有多套DCS合用功能，降低用户隔离成本；

（4）具有隔离站组故障检测报警系统，可以提升大型企业的管理效率；

（5）可以实现多台主隔离站合用1套备用隔离站，并实现全自动切换，大大提高了隔离系统的可靠性，降低冗余成本；

（6）经过大型石化企业长期应用的考验，系统运行稳定可靠；

（7）具有中国自主知识产权，在网络防护问题上可以不受制于人。

作者简介

王建（1957-），男，江苏苏州人。1982年毕业于华东化工学院（现华东理工大学）化工自动化与仪表专业，工学博士，留英博士后。现任北京优化佳控制技术有限公司董事长，长期从事工业自动化，工业过程在线优化，工业系统网络安全的技术和产品研发实施工作。

参考文献：

[1] ISACA.The State of Industrial Cybersecurity 2017[R].

[2] 吕建民. 工业系统信息安全现状与发展趋势分析[J]. 自动化博览（工业控制系统信息安全专刊第三辑），2016, 11.

[3] 王建. 一种本质安全远程数据监测系统及其监测方法[P].中国发明专利: ZL200610064971.8，2010－01－20.

[4] 谷俊涛. 工业控制系统安全研究现状[J]. 信息技术, 2017（7）.

[5] 李俊仁, 高兴彦, 张浩. 中国石油炼油与化工系统数采安全隔离设计[C]. 中国石油石化企业网络安全技术交流大会论文集, 2017, 06.

[6] 方咏梅, 刘志宏. 中小型实验装置联网工控安全解决方案[C]. 中国石油石化企业网络安全技术交流大会论文集, 2017, 06.

[7] 周业永, 王寅生. 本质安全型DCS数据隔离系统及其在工业上的应用[J]. 安全.健康和环境, 2011, 07.

[8] 何杨欢, 周博才. 本质安全DCS隔离站技术在工控数据采集中的应用[J]. 当代石油石化, 2013，21（9）: 30－33.