

工业控制系统的完整性与运行安全

ICS 系统的完整性管理——本文总结了目前 ICS 系统面临的挑战，阐述了如何利用国际石油企业证明的 PAS 独特的解决方案来强化 ICS 系统，以及从成熟的解决方案中获得的好处。

文 / 赵国玺

工业控制系统 (Industrial Control Systems, 是 SCADA、DCS、PLC、ITCC/CCS、SIS、F&GS、FCS 等系统的统称, 以下简称 ICS) 广泛应用于钻井、石油天然气、炼油、化工、造纸、冶金、食品、制药以及电力等关系国计民生的核心产业, 是现代企业生产控制的大脑中枢, 是企业实现自动化生产的基础, ICS 系统虽然

在整个企业的投资中看起来也许微不足道, 但 ICS 涉及生产安全风险的事件却非常之多。从上世纪 90 年以来, 由 ICS 系统被攻击引起的安全事故就一直存在, 有些在业界引起轰动, 这促使业界对 ICS 系统的安全问题进行严肃思考, 表 1 是几个典型安全事故的汇总。这些事故为企业带来严重的经

济损失和声誉损失, 为生产安全带来巨大的破坏, 也引起了对 ICS 系统 (OT : Operational Technology) 安全的严重关注。但这些事故能不能设法避免呢? 无论何种外部攻击或内部恶意行为, 对 ICS 系统的控制最后都是通过改变 ICS 系统的程序组态实现, 或者直接取得对 ICS 系统的操控权。如果我们能够对这

表 1 典型安全事故的汇总

时间地点	事故和后果描述	原因分析	备注
1999 年 美国贝灵翰姆	1999 年 6 月 10 日, 由 Olympic 和 Equilon 运营的贯穿华盛顿贝灵翰姆的油田管线破裂; 3 人死亡, 经理被判入狱, 3 600 万美元罚款, 6 100 万美元被用于安全花费。8 933 t 汽油溢出, 环境破坏, 设施修复费用以及公共关系噩梦。	事故的原因包括多种起因, 其中有一个原因就是美卓 METSO 的 SCADA 系统在危机中没能响应, 尽管调查人员不能够完全重复事故, 但结论表明 SCADA 系统数据库与离线检测的相比较被证明作了修改。	SCADA 程序组态被修改导致恶性事故; 内部风险
2000 年澳洲马鲁基多尔	2000 年 3 月到 4 月, 澳洲马鲁基多尔废水处理厂经历了多起错误引起废水倾入排水道。澳洲环境保护署描述: ‘海洋生物死掉、小溪变黑以及臭气让居民无法呼吸’。	在这个过程中, 一个曾经为该工厂工作的合同方。声称可以解决问题、讹诈政府。真实原因是他通过微波通讯入侵了该水处理控制系统。该人被逮捕后, 被判入狱 2 年	没有通过外网, 属于内网入侵事件
2010 年 伊朗超级工厂	导致铀浓缩最重要的设备 -- 数千台离心机毁损, 但同时送给操作员的显示正常。	Stuxnet 蠕虫病毒, 通过修改西门子 PLC 系统应用实现	Stuxnet 病毒修改 PLC 程序
2011 年 -2015 年	不同 HMI 供应商的用户被 BlackEnergy 恶意软件攻击, 该程序在大量产品例如 GE Cimplicity, Advantech/Broadwin WebAccess 和 Siemens WinCC 利用安全漏洞进行攻击。模块化程序能够侦测系统或破坏系统 (如通过 KillDisk 模块)。	2015 年 12, BlackEnergy 恶意软件被用于攻击乌克兰电厂, 该攻击影响了 22 万 5 千用户, 并不得不恢复手动操作以应对攻击。	通过攻击 HMI 来远程操控 ICS 系统。
2014 年德国	德国钢厂, ICS 系统阻止操作员去安全地关闭高炉。酿成恶性事故	SIS 系统程序被修改, 验收时与事故时的程序不一样	
2016 年 2 月。美国	Georgia-Pacific 造纸公司, 导致 ICS 系统停运, 严重伤害了生产能力。用户不得不花费很多时间修复整个系统。造成严重损失	被解雇前系统专家修改程序让员工们一天 24 h 不停地操作机器, 导致宕机和严重伤害生产能力	属于内部风险
2017 年 8 月, 沙特阿拉伯的皮特罗·拉比炼油厂	在中东导致意外停车 (非计划停车), 多套 Triconex SIS 系统和 DCS 系统遭到破坏	TRITON/TRISIS 将恶意代码写入 SIS 系统内存, 它似乎是通过将 SIS 重新编程以允许不安全状态, 然后使用 DCS 创建不安全状态或危险来准备进行攻击。	

PROCESS-Tip

* 更多信息请扫描二维码:

chem.vogel.com.cn

* 反馈编码: A200925

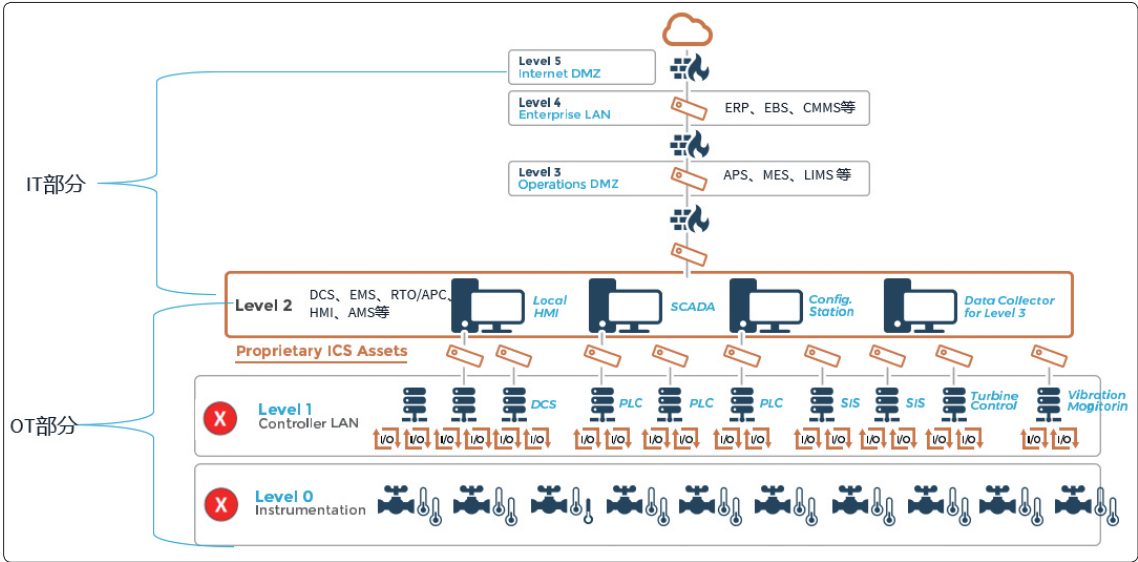


图 1 现代企业典型系统架构 (ISA99)

些修改进行识别，用户的 ICS 系统程序被修改（无论是外部攻击所致、或是病毒感染、员工失误、亦或是员工 / 服务商人员恶意修改），就有可能避免这类事故的发生。

ICS 系统运行现状

随着工业 4.0、IIOT、智能工厂、中国制造 2020 以及两化融合的快速推进，ICS 系统的孤岛现象彻底消失，其开放性带来的风险也与日俱增，图 1 是现代企业最典型的系统架构：

如图 1 所示，现代企业的 IT 与 ICS 系统部分的集成不可避免，而企业由此面临的安全风险状况也变得愈加复杂，因此从企业的董事会到生产运营基层部门，ICS 系统的运行管理与安全越来越成为现代企业生产安全不可回避的一个重大课题。

Kaspersky（卡巴斯基）在 2016 年发布的报告，披露了绝大

多数组织的 ICS 系统面临威胁，该研究对 188 019 套 ICS 系统进行调查，发现 91.1% 的系统存在漏洞，可以被远程控制或利用，超过 87% 的系统具有中等风险漏洞，7% 的系统具有严重安全漏洞。

而来自 ICS-CERT、Kaspersky Lab、IBM-X-Force Research（2016 年）的分析数据表明，ICS 外来威胁占到大约 39.2%，而来自于内部的威胁则占到 60%（其中 45% 属于恶意行为，15% 属于人工失误范畴）。

到目前为止，尽管在对 OT 技术安全方面有了很大的进步，但主要能够提供的方案还是基于 IT 技术的解决方案：

- 防火墙；
- 网闸；
- 漏洞扫描；
- 白名单；
- 防病毒软件；
- USB 禁用和其他一些应用禁用策略等。

ICS 系统优点是：典型的周界防护，针对 L5-L2 层，如图 1；防止外来攻击，容易理解容易实施；

对已知的攻击方式有效。

但也存在一些缺点：对未知的攻击无法进行预测与防护；对系统本身存在的安全漏洞和缺陷无能为力 L2-L0；对内部风险管控无能为力。

网络安全的特点是，道高一尺、魔高一丈，因此以 IT 安全技术为中心的解决方案无法真正解决 ICS 系统的管理和安全问题，比如 Stuxnet 病毒在造成破坏之前，杀毒软件的病毒库根本没有它的特征进行识别；再比如，很难预测以后黑客会以什么样的方式和手段进行网络攻击；另外，工业过程环境中的漏洞扫描和评估也具备危险性；扫描或连接到敏感设备来收集漏洞数据可能会导致无法接受的生产中断，给生产带来损失。

经过几年的项目实践，国内 ICS 系统除了面临外部攻击之外，面临的最主要问题和风险如下：

- 控制系统种类多（DCS、PLC、SIS、RTDB 以及 Intouch 等）、地理分散，管理难度大，人员流失导致导致系统专家超负荷工作；

本文作者系 PAS 中国区经理。

• ICS 系统本身是否有潜在风险；

• ICS 系统的管理、维护以及运行安全等面临很大挑战；

• 控制系统上线后，由于不停的组态变更或增加新的内容（硬件、控制策略等），用户对当前系统中运行的程序内容认识会越来越有偏离，技术人员往往对此潜在风险束手无策；

• 对控制系统的修改无法进行自动记录与追踪；

• 对非法修改无法进行自动识别和追踪，没有有效办法实现对系统的风险管控；

• 对控制系统的安全漏洞和组态 / 逻辑缺陷没有有效的检测能力；

• 缺乏对 ICS 系统本身故障的远程诊断与分析能力；

• 大修期间极易产生系统组态修改带来的风险，缺乏手段跟踪与识别这些风险；

• 不同 ICS 系统之间的数据链路是否一致，有无可能引起事故的错误。

对于上述问题，仅靠基于 IT 的方案是无法进行解决的，因此 ICS 系统的安全需要把基于 IT 技术的周界保护技术和基于 OT 的本质安全解决方案有机结合起来，才能更好地对 ICS 系统的风险进行管控！

为此在现代企业产生了一个新的职位：CISO (Chief information security officer)，即首席信息安全主官，集合 IT 和 OT，解决信息安全、控制安全和生产安全问题。

OT 和 IT 系统之间的连接正在激增，极大地增加了网络攻击的一次攻击成功的可能性；而且风险不仅仅是确保数据的保密性、

完整性和可用性，更重要的是要保护 ICS 资产免受网络攻击，以保护人员安全、环境以及工厂生产率 and 盈利能力。CISO 面临的另外一个挑战就是，每个企业不同供应商、不同种类以及不同位置的 ICS 系统，每个不同的系统运行的是各自不同的专业软件。

因此通过 IT-Centric 解决方案和 OT-Centric 解决方案相结合，才是真正解决企业工控系统运行管理与安全的有效途径，因为基于 IT-Centric 解决方案，有很多公司提供且非常成熟，此处不进行展开，本文将对 OT-Centric 方案进行讨论。

基于 OT 的技术方案

完整性是可靠性和安全性的基础，设备完整性、管道完整性、储罐完整性以及数据完整性等是企业生产智能化的重要组成部分，但在所有的资产完整性解决方案里面，几乎看不到对 ICS 系统的完整性管理的描述。主要原因是：

- ICS 系统的种类、品牌多；
- ICS 系统专业性高，私有技术多；
- ICS 系统复杂程度高、特别是系统之间的复杂逻辑和通讯关系；
- ICS 系统直接与生产相关，一旦有问题风险更大；
- 数字化难度大；
- 缺乏有效的工具。

ICS 系统的数字化与在役库存管理

非常简单的一个道理，如果你想保护你的 ICS 系统，首先你要能够看到你的 ICS 系统，清楚地知道 ICS 系统的所有资产细节，这是你能够保护 ICS 系统资产的前提；ICS 系统的资产包括 ICS 系

统的软件、硬件等，但最核心的是你的控制策略（组态），因为控制策略才是真正驱动生产自动化的核心，事实上，你可以选择任何 ICS 系统实现同样的控制策略。

以 DCS 系统为例，从设计到组态完成、再到现场调试、开车，进入正常生产，小的改动、修正以及回路的增减等一直不断进行，随着时间的推移，这将导致装置工程师对 DCS 系统的认知与实际情况产生越来越大的认知偏差甚至错误。而这种认知偏差 / 错误将是很大的隐患。而消除工程师对实际 ICS 系统的认知偏差，就需要能够对 ICS 系统的在役库存进行监测，对每个控制器、每个卡件、每个卡件的每个通道、每个接线端子以及每个控制策略的情况了如执掌，比如它们软硬件版本？在哪个位置？起什么作用？如果它们有问题会带来什么后果？等等。

要做到能够具备对 ICS 系统的透视能力，首先我们就需要对 ICS 系统进行数字化，即把 ICS 系统原样不动进行数字化解析（提取 ICS 系统内存里面运行的数据），如图 2 所示：

把不同品牌、不同种类、不同位置的 ICS 系统进行数字化，通过一个统一的单独的平台对它们进行监管，不但可以实现 ICS 系统的动态台账管理，还能实现对 ICS 系统的风险预测，避免非计划停车。

上述这些系统的硬件、软件、版本、相互联系以及控制策略等都透明可见。对 ICS 系统所有的构成都可以分类进行查询和汇总，对所有的改变都可以自动感知。

ICS 系统风险评估

ICS 系统的而数字化，让我们准确无误地透视真实的 ICS 系

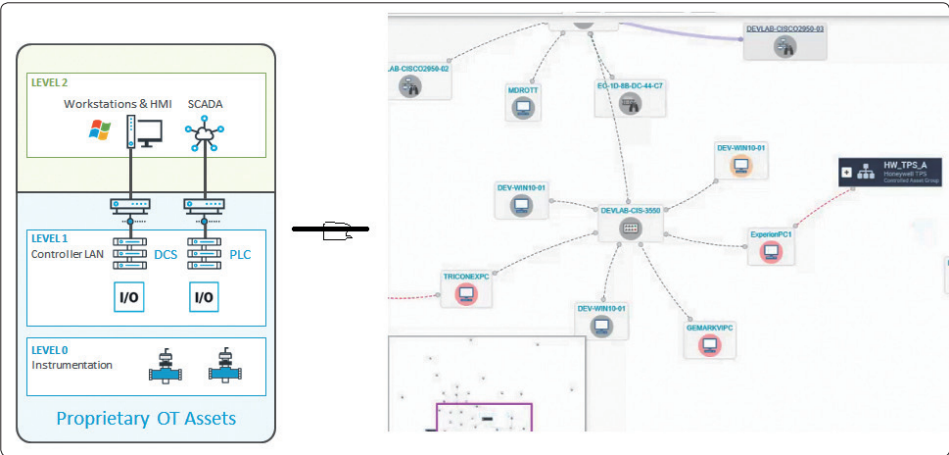


图 2 ICS 系统数字化

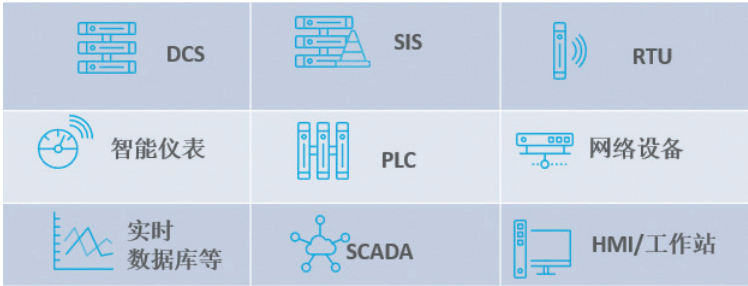


图 3 典型的 OT 资产

统的情况，这位我们对 ICS 系统进行风险评估打下基础。

1. ICS 系统的安全漏洞自动检查

基于 IT 技术的方案的漏洞检测主要还是对 HMI/ 工作站即 L2 层进行漏洞检测，但不具备对 L1-L0 层的漏洞检测能力。

ICS 系统的漏洞检测，不但要包括 L2 甚至 L3 层的漏洞检测，还同时能够对 L1-L0 层软件 / 设备进行漏洞检测。

以检测 ICS-CERT 发布的漏洞为例，对检测到的漏洞同时显示其 CVSS 分值，以便用户可以直观地得到当前 ICS 系统的危险程度。

因为今天检测不到的新漏洞，也许会在几个月后被发现，因此对安全漏洞的检查必须自动完成，要具备对漏洞库进行更新的机制。

2. ICS 系统的组态缺陷检测

对当前 ICS 系统的组态进行缺陷分析与 汇总，帮助用户发现丢失的位号、识别相互矛盾的组态数据等，组态缺陷可以根据情况进行定制。

比如，安全边界冲突就是组态缺陷的一种，如果报警值比连锁值还高，则非常容易造成在没有对报警处理的情况下出现停车，即非计划停车，而非计划停车带来的经济损失和环境损失往往是巨大的。

在一个几万点或十几万点的工厂，人工进行这类缺陷的检查是不可想象的，因此，定义缺陷属性，对组态进行自动大数据分析，是可以快速发现缺陷问题的真正有效的手段。

3. 数据链的检查

现在数字化设计交付已经成

为常态，数字化交付之后，工程师进行 ICS 端组态、先进控制、HMI 以及 MES 需要与 ICS 集成并采集数据以及以 ICS 系统与 MES 系统的集成为例。由于 MES 与 ICS 往往是不同厂家的产品、由不同的团队分别完成，由不同的团队进行维护，因此 ICS 系统与 MES 系统的组态一致性就容易出现偏差，导致 MES 采集数据的不准确。因此需要对系统之间的数据链路进行校对，确保一致。如图 4 所示。

组态管理与非法修改的识别与定位

ICS 系统的组态变更主要由如下几种情况：

- 黑客侵入修改；
- 靶向病毒感染引起修改（如 Suxnet 针对 Siemens PLC、Tricon/ TRISIS 针对 Triconex SIS 系统）；
- 未经批准的恶意修改；
- 经过批准但由于疏忽导致错误修改。

其实无论哪种修改，只要我们能够知道 ICS 组态被修改、什么地方被修改以及修改前后的不同之处，那么这种修改就很难对实际产生大的风险。

1. MOC 管理

现在大多数用户对 ICS 系统的变更与修改都有严格的规定，主要的问题是如何完善地执行这些规定。线下规则对恶意修改或人工疏忽导致的错误修改其实是无能为力的。因此，再好的规则，没有执行监督也是没有办法保证执行效果的。

因此结合用户的变更规定，将其进行客户化定制，把之前的线下变更要求提交、审批等变成动态的线上执行，这样就可以对用户的变更进行记录、跟踪、回溯、

领先的

智能阀门定位器/ 调节阀 供应商

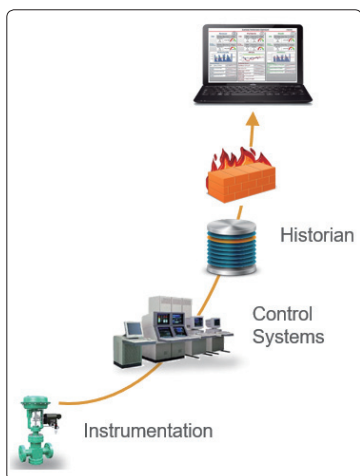


图 4 保护数据链路的正确

汇总以及比较等，帮助用户识别非法修改、并定位非法修改（无论是黑客所为、病毒所为或未经授权的恶意所为），而对方修改则可以直接把处理任务分配给相应的工作人员进行处理，并对处理过程进行记录追踪，从而完成内部风险管控。

无论是对于点组态的修改、逻辑或程序的修改，还是流程图的修改等，都应该可以进行识别。

2. 基准管理

通过基准管理可以进行阈值设置，即对比较重要的组态内容的变更提供限制，避免变更带来的风险；阈值设置后，一旦提交的变更值超过阈值，则审批人会自动得到风险提示，以避免进行错误的审批。

跨系统控制关系描述（Control Map）

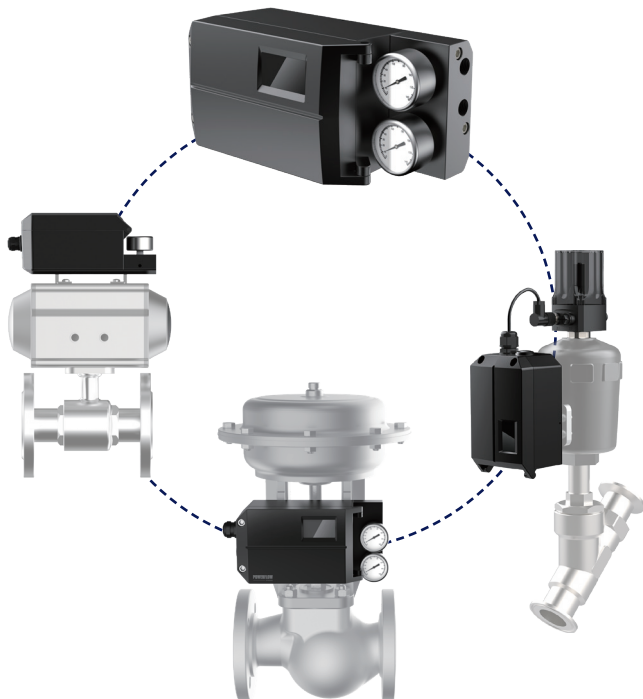
通常在一个系统中，位号 / 设备之间的逻辑关系是相对容易弄清楚的，但如果不同系统之间存在逻辑关系或相互引用关系，要搞清楚就不是一件容易的事情了。

比如在 SIS 和 DCS 系统之间、DCS 和实时数据库之间、DCS 和 APC 系统之间，如何快速描绘它们中的位号之间的相互关系呢？

这就需要对系统之间的通讯协议进行解析，比如 OPC 通讯，存在着一个位号之间之间的映射表，ModBus 通讯，存在着一个地址映射表，如果对这些进行了正确解析，则它们之间的相互调用关系及数据流向就可以自动描绘出来，如图 5 所示：

这样，用户可以非常容易地追踪跨越从现场仪表到 DCS/PLC/SIS/RTDB/APC/MES 等的信号流图谱，自动生成针对每个对象（位号 / 设备）的业务树 / 逻辑树，直接和间接关系，帮助用户快速进行故障处理。同时，可以作为应急预案的辅助设计。

数字化交付，对设计院提供的 SPI 数据库进行解析，生成如图 6 所示的从仪表到端子柜到安全栅柜到 DCS 端子接线、到 IO 卡通道位号以及到控制器控制算法模块位号之间的全程关联关系，而且能够和现场进行同步变更，这是对 ICS 系统从现场到控制室的真正的完整性管理。



- **高品质**，核心器件采用原装进口。
- **重服务**，质保期 24 个月，12 个月内出现质量问题倒赔 2000/ 台。
- **易使用**，匹配市面上所有的气动调节阀，并可实现一键自整定。
- **多功能**，具备 HART 通讯，过程控制等丰富附加功能。



杭州博流科技有限公司
地址：浙江省杭州市西湖区西园八路 11 号
数字信息产业园
电话：+86-0571-88969132
E-mail: Jackiewu@powerflow-tech.com

广告

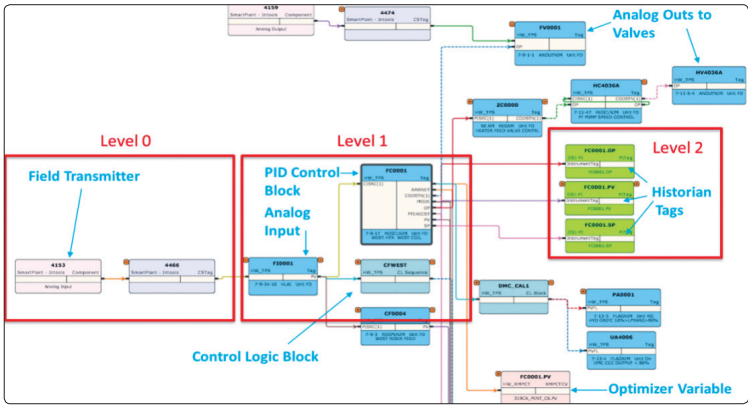


图 5 自动生成跨系统控制关系

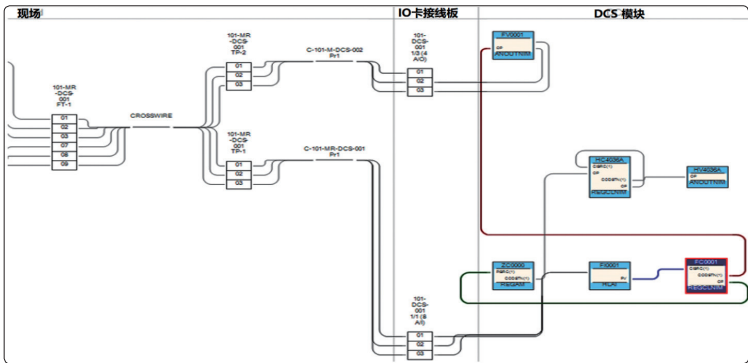


图 6 全回路数字化

交叉引用追溯

在 ICS 系统中,位号、文件(流程图等)都存在交叉引用的情况,对这些内容进行完全解析与追踪,可以帮助用户发现有价值的信息。

比如,搜寻 FC1001 这个位号,可以自动显示与 FC1001 相关的流程图名称、操作组名称、报表名称、相关接线图名称、其他系统如实时数据库等以及文档文件如仪表规格文件名称等。而通过这些名称,用户就可以直接打开这些文件。比如通过位号就可以查到回路所关联的仪表与阀门的详细规格材料、接线图等。

支持随时查询到所有用户感兴趣的内容,使得对特定对象的理解异常容易。

对 ICS 系统工作站的管理

现实中,每个工厂的工作站

(DCS 工程师站、操作员站、OPC 服务器、SIS 系统的 HMI 工作站、OPC 服务器等以及 PLC 系统的 HMI 工作站等)几百上千台甚至更多,几乎没有哪个工程师能清楚知道:每个工作站安装软件的具体信息如操作系统哪个版本?打过什么补丁?工作站安装了哪些应用等。但工作站作为 ICS 系统的重要部分,用户需要对它们有充分的了解,比如对操作系统和账户管理、追踪和记录不同账户的行为动作等。

我们对 Windows 的注册表等相关信息的解析,结合之前 Windows 的漏洞库,就可以自动对工作站是否面临如勒索病毒感染的风险进行判断,并把有风险的工作站直接推送给相关管理人员进行风险排除的工作安排,且对其进行记录与追踪,大大节约

了工作人员的工作量并指明工作内容和方向。

比如,工作站做了 USB 禁用策略,一旦有人通过 USB 访问工作站,都会被记录。

比如,一旦有人安装了程序、即使做了卸载,依然可以被记录下合适安装、合适卸载的全部信息。

对 ICS 系统的数据备份和恢复

对 ICS 数据自动定期进行备份,以保障数据的有效性和系统恢复的可靠性;保持完整的 IT 存货和 OT/ICS 组态数据资产存库,包括控制策略、I/O 卡件、硬件以及安装的软件和任何用户自定义数据等,这样一旦系出现崩溃等严重问题,这些数据可以帮助用户进行系统快速恢复。

同时,ICS 系统数据的自动备份可以在线存储、也可以同时进行离线存储,万一受到勒索病毒类侵害,也可以通过备份的系统数据进行系统恢复,避免更大的损失。

总结

ICS 系统的完整性管理是实现 ICS 系统本质安全的前提,传统的基于 IT 技术的解决方案是解决 ICS 系统周界保护的有效办法,但无法解决 ICS 系统的本质安全问题,因此,利用 ICS (DCS/SIS/PLC/ITCC/CCS/FGS/RTDB 等)系统专业知识,即采用基于 OT 的解决方案是真正解决 ICS 系统完整性管理、运行安全以及远程维护支持的正确手段!