

设备物联网系统建设 及工控安全实践

文/北京兰光创新科技有限公司 朱铎先



朱铎先

北京兰光创新科技有限公司董事长

随着德国工业4.0、美国GE工业互联网以及中国智能制造战略如火如荼地推进，引发了以新一代信息技术与制造业深度融合为特点的全球性新一轮工业革命。工业互联网通过网络、平台、安全三大功能体系，实现人、机、物全面互联，形成智能化发展的新兴业态和应用模式，是新一轮工业革命的关键基础设施。制造企业如果能抓住工业互联网发展机遇，构建安全、先进的工业互联网系统，可以很好地促进企业智能化转型升级。

设备互联是重要基础

纵观德国工业4.0、日本工业互联网等战略以及美国GE工业互联网，无不把设备互联作为工业互联网的重要基础。

从工业互联网角度看，德国工业4.0通过三步走的策略构建工业互联网系统。纵向集成实现企业内部的集成，包括设备与设备之间、信息化系统之间、信息化系统与设备之间的集成，这是后续两个集成的基础；端到端集成是围绕产品生命周期企业间的集成，在此阶段已经引入互联网要素；横向集成是以价值网络为主线，不同企业间之间的集成，是社会合作的重要基础，是广义上的工业互联网概念。

作为工业互联网联盟的发起单位，通用电气（GE）在工业互联网概念中，更是明确了“通过生产设备与IT相融合，目标是通过高性能设备、低成本传感器、互联网、大数据收集及分析技术等组合，大幅提高现有产业的效率并创造新产业”。“生产设备与IT相融合”与德国工业4.0纵向集成有异曲同工之处，车间层面的设备互联互通是其重要组成部分。

2017年，在参考德国工业4.0、GE工业互联网等战略基础上，日本经济产业省提出“互联工业”战略，并定为日本国家级发展愿景。“互联工业”就是希望在全球物联网（IoT）和人工智能（AI）崛起的过程中，“通过连接人、设备和技术等实现价值创造的互联工业”。

据日本经产省2016年调查显示，有40%的日本工厂在2015年前就已经实施了设备联网与数据采集，到2016年，这一数字就提升为66%，其中大型企业达到了88%。而形成对比的是，我国企业2015年数字化设备联网率仅为32.1%，不及日本的一半。

“中国制造2025”中也强调指出：“促进制造工艺的仿真优化、数字化控制、状态信息实时监测和自适应控制。”生产设备互联互通是智能制造的重要基础。

由此可见，打造以生产设备互联为核心的设备物联网系统，对生产设备实现互联互通、大数据分析可视化展示，实现数字化、网络化、智能化的管控，是制造企业实施智能制造的关键一环，也是构建工业互联网系统的

重要组成部分。

设备单机工作存在风险

在工业互联网三大体系中，网络是基础，平台是核心，安全是保障。下面从制造企业视角谈谈生产设备网络化的数据采集及工控安全。

以数控加工车间为例，随着数字化设备的增加，这些高、精、尖设备在生产中发挥了重要作用，但由于在程序传输、程序管理和设备管理等方面还停留在传统的工作方式，不仅影响了设备效率与产品质量，在工控安全方面也存在很大隐患：

1) 程序通信采用笔记本单机传输形式，频繁的热插热拔容易烧坏机床或计算机接口。

2) 有些企业采用U盘复制程序形式，U盘的频繁使用增加了病毒、木马传播的概率。

3) 编程员缺少数值处理、模拟仿真和版本比较等数控编程专用软件，加工程序容易出错，就可能发生撞刀、撞机等情况。

4) 程序分散在程序员手中，无严格的流程签署管理，容易调用

不正确的程序或版本，对产品加工质量及生产设备存在安全隐患。

设备状态不能自动采集，出现设备故障、工人违规操作等情况，相关人员不能及时获知，快速响应处理，不仅影响正常生产，并且容易对设备造成更大的损害。

兰光设备物联网系统是北京兰光创新科技有限公司基于十多年设备联网研发及实施经验，在600余次航空航天等成功案例的基础上，以“中国制造2025”为宗旨，参考德国工业4.0及美国GE工业互联网等先进理念，为中国制造企业量身打造和设备智能化互联互通系统。本系统既包括传统意义上的DNC（机床联网）、MDC（机床监控与数据采集）等功能，也包含对热处理设备、机器人、AGV（自动导引运输车）和自动化立体仓库等各类数字化设备的智能化管控，是工业互联网在制造企业的具体应用。请见图所示。

系统管理的主要对象为制造企业的各类数字化设备，如CNC数控机床、各类压铸等成型设备、机器人、热处理设备和AGV等，

通过以太网卡、RS232与RS485等各类通信接口，MODBUS、PROFINET、PROFIBUS及CC-LINK总线等不同接口形式，用一台服务器对这些生产设备进行互联互通，实现程序的集中管理、网络化传输、数据自动采集、大数据分析 and 可视化展现等功能，并通过联接底层各类设备、生产线与上端管理系统，实现软件—软件、软件—硬件、硬件—硬件三项集成。

通过实施设备物联网系统，不只是在生产效率与产品质量得到很大提升，在工控安全方面也会带来很明显的改善：

1) 通过构建基于以太网的设备网络，实现设备的网络化集中管理与控制，从根本上杜绝了U盘、CF卡等传输不安全的工作方式。

2) 专业的版本比较、程序仿真、数据处理等功能可把程序错误消除在虚拟环境中，确保工控设备的安全。

3) 完善的程序签署流程，精准的权限管理，方便的版本管理，从而有效地避免因调用程序错误而造成撞刀、撞机等情况。

4) 设备状态的实时采集与分析，可及时了解设备状态、工人操作规范情况，确保设备安全。

5) 通过大数据分析功能，对设备进行历史故障查询、故障时间分布、故障概率分布和设备故障预测等，确保设备安全、健康地运行。

6) 设备实现网络化管控后，设备外设接口实行封禁，并在设备网络内部部署行为安全审计设备，既能降低外部移动存储工具对设备主板的损坏，又能防止涉密信息的泄露。

设备互联系统层面的安全隐患

设备物联网系统可以有效地解

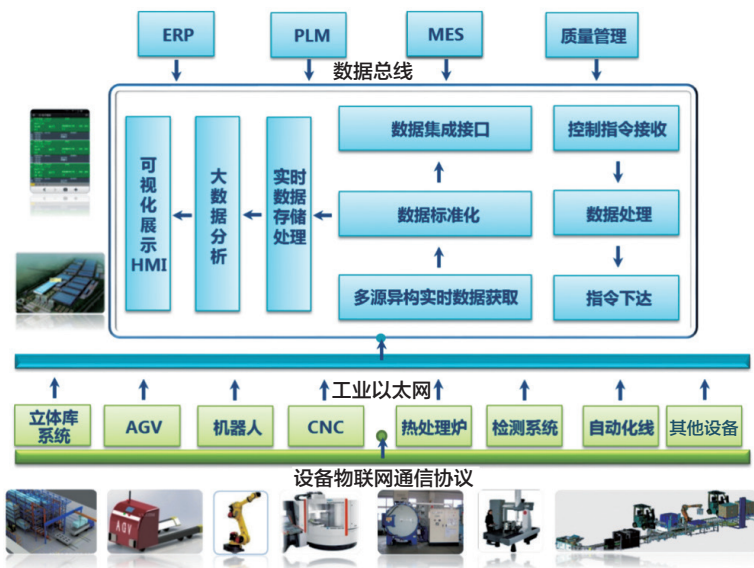


图 兰光设备物联网系统

决单机设备的安全问题，但同时由于网络连接带来了系统层面的安全隐患。从安全角度来说，设备联入网络，就增加了被病毒或不法分子大面积攻击的可能，有可能给企业带来严重损失。

2010年的“震网(Stuxnet)”病毒是非常著名的工控安全事件。这是第一个专门定向攻击工业系统的蠕虫病毒，它利用Windows系统和西门子数据采集与监控系统的多个漏洞进行攻击，能够定向破坏工业关键设备。由于被“震网”病毒控制，伊朗布什尔核电站1/5的离心机被损毁，纳坦兹核电站8 000台离心机中有1 000台也被先后换掉。专家估计，“震网”病毒使伊朗核工业技术水平倒退十年。

据美国网络安全公司FireEye发布的《2016工业控制系统漏洞趋势报告》数据显示，2015年相比2014年，安全漏洞增加了49%。截止2016年初，全球已发生300余起针对工业控制系统的安全攻击事件。

现在，对工业控制的攻击与数据窃取已呈常态化、高频化。

设备物联网系统工控安全实践

工业互联网系统除了具有强大、稳定、可靠的业务功能外，安全保密也是一个重要的衡量标准，不能只考虑系统的业务需求、系统性能、技术路线等因素而忽视系统自身的安全性。由于客户主要集中于军工、大型机械制造等高端企业，用户对安全性的要求非常严格，兰光创新在工控安全方面进行了大量的研究与实践，并取得了较好的应用效果。以下是兰光创新近些年的一些实践，分别从网络安全、设备安全、主机安全、应用安全和管理制度等几个方面与大家分享，希望抛砖引玉，共同为

工业互联网安全、健康发展而尽一份绵薄之力。

1. 网络安全

网络是基础，网络安全是整个系统安全的前提。在网络安全方面采取的措施主要有：

划分安全域，利用VLAN、ACL等技术按部门或职能划分成不同的安全域，通过权限分配控制访问等手段；隔离技术，在设备内网与企业高涉密办公网之间，通过防火墙、网闸、VPN等各种安全隔离设备以及严格的访问控制；识别审计，通过主机审计系统对于接入系统的终端进行身份识别认证和鉴别，防止非法设备接入网络；入侵防护，通过部署入侵防护系统，可自动对网络通讯行为进行分析，实现对网络攻击的监测和分析；边界防护，按国家涉密等级划分，设备物联网/SCADA等系统为低密级工控网，应采用专用的物理网络以及有效的安全防护措施；身份登录鉴别，如果条件允许，可采用智能卡+PIN码、生物认证技术（指纹、虹膜等）等更安全的登录方式。

2. 设备安全

作为设备物联网系统中的主体，设备自身的安全也非常重要。包括：对设备数控系统进行严格防护、禁用设备外设接口、设备端口绑定。

3. 主机安全

对于主机及配套的外设硬件要关注以下五个方面：

1) 服务器和主机建议采用国产知名品牌设备，主机操作系统和数据库系统软件采用正版操作系统。

2) 关闭和禁用系统提供功能服务和网络服务以外的通信端口和服务功能项。

3) 在系统中部署主机安全审

计系统，对产生的日志记录进行定期的备份和分析。

4) 对系统管理权限的口令管理采取最高级别的安全管理，如密码复杂度、定期更换和用户登录超时/超次自动锁定等安全手段。

5) 采用双机部署原则：一方面实现系统故障的快速高效切换，另一方面可实现数据的安全冗余备份和快速恢复功能。

4. 应用安全

在应用安全层面，要注意以下三个方面：

用户的角色划分和权限分配管理。通过应用系统角色的权限管理功能，不同的人员设置不同的权限访问不同密级的资源，实现系统高效、有序、安全管理。

系统数据库安全。对数据库访问管理权限进行严格划分，并有详细的操作日志记录。

对于涉密企业系统管理安全，遵循企业更为高级别的安全保密要求，实现三员分立管理，即系统管理员、系统保密员与系统审核员三权分立，各行其权。

5. 健全的管理制度

工控系统的安全保密是“三分靠技术，七分靠管理”。将技术、管理与标准规范制度结合起来，以安全保密策略和服务为支持，形成信息安全保密工作的能力体系。以防护、监测、响应、恢复为核心，对涉及安全保密的相关组织和个人进行工作考评，并结合标准化、流程化的方式加以持续改进，使企业信息安全保密能力不断提高，确保企业安全生产及工控系统的安全。

安全无小事。道高一尺，魔高一丈，工控安全是个不断完善、不断提高的过程，一定要引起我们的高度重视与积极行动，为工业互联网健康发展提供安全保障。EA