直流电源 IC200MDL750 GE通用电气 诚信经营质量可靠

产品名称	直流电源 IC200MDL750 GE通用电气 诚信经营质量可靠
公司名称	厦门盈亦自动化科技有限公司
价格	633.00/件
规格参数	品牌:GE 型号:IC200MDL750 产地:美国
公司地址	厦门市集美区宁海三里10号1506室
联系电话	0592-6372630 18030129916

产品详情

直流电源 IC200MDL750 GE通用电气 诚信经营质量可靠

IC200NDD010	IC200CHS014	IC693CBL327
IC200UDD212	IC200UDD020	IC693MDL260
IC200PNS002	IC200NDD101	IC693CBL311
IC200CHS102	IC200CHS011	IC693CBL303
IC200CHS101	IC200CHS122	IC693CBL313
IC200UDD220	IC200MDL743	IC693NIU004
IC200UDR120	IC200MDL750	IC693CBK004
IC200CPU005	IC200CBL655	IC693MCD001
IC200UDD240	IC200CHS001	IC693MDL241
IC200CHS112	IC200CBL602	IC693PBS201
IC200CHS022	IC200CHS015	IC693CBL301
IC200PKG104	IC200CBL635	IC693CBK002
IC200NDR010	IC200CBL615	IC693CBK001
IC200UDD104	IC200UAL006	IC693MDL330
IC200NAL110	IC200MDL742	IC693PBM200
IC200PNS001	IC200UDD040	IC695RMX128
IC200NAL211	IC200MDL740	IC695CPU320
IC200NDR001	IC200CHS002	IC695CMX128
IC200MDL930	IC200CBL555	IC695ACC415
IC200CHS025	IC200CBL605	IC695ACC414
IC200CHS005	IC200UDD110	IC695ACC413
IC200CHS006	IC200MDL730	IC695CPK400
IC200CHS003	IC200CBL600	IC695EDS001
IC200CHS111	IC200CBL510	IC695ACC412

IC200MDL940	IC200CBL545	IC695CPE302
IC200CPU002	IC200CBL550	IC695CDEM006
IC200UDD112	IC200UAR028	IC695CPL410
IC200UDD120	IC200CBL525	IC695PNS101
IC200DEM103	IC200MDL741	IC695ALG626
IC200UDD064	IC200UAL005	IC695ALG608

直流电源 IC200MDL750 GE通用电气 诚信经营质量可靠

01 工业控制系统典型架构与现状

工业控制系统典型架构

工控系统的主要目标是实现工业自动化生产线的物流控制、设备信息监控及诊断处理，其主要功能包括设备管理、任务管理、日志管理、调度管理、诊断管理、系统仿真等。

工控系统通常包括，制造执行系统（MES），监控和数据采集（SCADA）系统，分布式控制系统（DCS），可编程逻辑控制器（PLC）等组件。MES系统主要对生产过程进行管理，如制造数据管理、生产调度管理、计划排程管理等。SCADA系统通常使用中心化的数据采集和监控手段来控制分散的设施。DCS系统通常用于控制本地区域内的生产系统，例如监控和调节本地工厂。PLC通常用于特定的离散设备，提供相应的调节控制。工控系统还涉及远程终端（RTU），智能电子设备（IED）以及确保各组件通信的接口技术。

工控系统还包含控制循环、人机接口（HMIs），和使用一系列网络协议构建的远程诊断和维护工具。工控系统广泛应用于各行各业，如电力、能源、化工行业、运输、制造（汽车、航空航天和耐用品）、制药、造纸、食品加工等。

由于工控系统应用的技术领域、行业特点以及承载业务类型的差异，工控系统的架构亦会不同。在典型的工控系统中，一般包括四个层级：现场设备层，现场控制层，过程监控层和生产管理层（层级0-层级3）。其上层生产管理层与企业资源层中的ERP软件对接（图一）。

工控系统的信息安全隐患分布于工控系统架构的所有层级。攻击者可能通过嗅探、欺骗、物理攻击及病毒传播的方式，进行以下未授权或非法操作，影响企业正常生产：

获取并分析各层级设备中的信息；

修改存储于工控系统组件中的敏感信息；

获得存储于工控系统组件中的用户凭证，冒充合法用户；

发布错误指令或进行错误配置；

传播恶意代码造成不必要的系统停机和数据破坏；

通过社会工程(Social Engineering)获取用户信息。

工控系统不同于传统IT系统。相比于IT系统，工控系统拥有以下特性：

系统对延时的忍耐度较低，对可靠性要求高，大多需要全年不间断工作；

部分工控系统仍旧使用陈旧的操作系统（OS），因此对此类系统的安全管理要求更高；

由于工控系统涉及软件、硬件、固件及工艺流程，因此其变更管理更为复杂；

系统通讯协议更为混杂，包括各种工业总线，工业以太网，无线接入，射频和卫星等；

系统整体架构更为繁杂，企业安全认知度和安全意识相对较低；

从风险角度看，除了传统信息安全以外，工控系统安全还需要关注人身、环境、生产以及物理等方面的安全；

系统生命周期更长，对系统设计完备性、工艺集成性要求更高等。

综上，相比IT系统，建立涵盖工控系统各层级的信息安全体系更为复杂，需要企业管理层的重视和监管，以及企业内跨部门的协作。

工业控制系统安全现状

一直以来，企业信息安全的防护措施主要集中传统IT系统，特别是面向公众的系统和服务。针对工控系统的信息安全问题，企业往往采取模糊即安全（security by obscurity
）的被动方式，未给予足够的关注和重视。

根据CVE（Common Vulnerabilities and Exposures）的统计显示（详见图二），2011年起工控系统漏洞的发布数量显著增加，并且发生针对工控系统的安全事件，其中影响较大有：2010年伊朗核电站的震网病毒攻击导致铀浓缩设备故障事件，2015年的乌克兰大规模停电事件，2018年台积电生产基地被攻击的事件，以及2019年委内瑞拉的电网被攻击导致全国大部分地区断电事件。这些事件都造成了十分严重的后果。

根据2015年美国国家标准技术研究所（National Institute of Standards and
Technology，NIST）的调查结果*，工业控制系统可能面临的安全事件主要有：

阻塞或延迟通过工控系统网络的信息流，中断工控系统的运行；

未经授权的篡改指令、命令或警报阈值，损坏或关闭设备，造成环境影响以及威胁人身安全；

向系统管理员发送不当信息，以掩盖未经授权的更改，或引起操作员采取不适当行动；

工控系统软件或配置被非授权修改，或软件被病毒或恶意软件感染；

干扰设备保护系统的运行，危及昂贵且难以更换的设备；

干扰安全系统的运行，危及人身安全。

（*Source：Guide to Industrial Control Systems Security，2015，NIST）

依据普华永道中国的追踪和研究，我们发现企业缺乏有效的管理和技术措施保障工控系统的安全，存在较多安全隐患。诸如：

操作系统的安全漏洞；

防病毒及恶意软件的管控漏洞；

使用U盘、光盘等外接设备的管控缺失；

设备维修时，笔记本电脑存在随意接入的情况；

工控系统网络边界防护不充分；

访问和接触控制（包括远程访问、管理维护）薄弱；

工控软件生命周期的安全管理漏洞；

缺乏安全事件应急响应机制。

直流电源 IC200MDL750 GE通用电气 诚信经营质量可靠