通讯模块 IC693MDL230 控制卡 调试方便

产品名称	通讯模块 IC693MDL230 控制卡 调试方便
公司名称	厦门盈亦自动化科技有限公司
价格	888.00/件
规格参数	品牌:GE 型号:IC693MDL230 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

通讯模块 IC693MDL230 控制卡 调试方便

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

通讯模块 IC693MDL230 控制卡 调试方便

工控系统安全体系建议

综合上述主流国家和地区以及国际组织发布的关于工控系统安全的要求、标准和指南，普华永道中国建议应用工控系统的企业，建立和实施适合的工控系统安全防护体系以应对工业控制系统安全风险。企业建立工控系统安全体系可参考以下模型（图二）。

04 工业控制系统安全风险与防护

工控系统安全脆弱性

依据《信息安全技术 网络安全等级保护基本要求》(GB/T 22239-2019)，工控系统分为生产管理层、过程监控层、现场控制层和现场设备层，涉及多种组件、应用和通信协议等，若一个环节保护不到位，就有可能导致整个工控系统被攻击而影响生产。脆弱性涉及管理层面和技术层面：

管理层面脆弱性包含：安全策略和制度不完善、安全职责不明确、安全意识薄弱、安全宣传与培训不完善、管理监督不到位、供应链管理机制欠缺、数据保护和备份管理不足、应急响应机制缺乏等；

技术层面脆弱性包含：安全架构设计不合理、操作系统陈旧、安全补丁不及时、访问控制不恰当、病毒或恶意程序防护不当、通信协议不安全、网络边界防护不足、系统配置不恰当、物理和环境保护薄弱、日志缺失或保留时间过短等。

工控系统安全威胁

威胁可能来自企业外部或内部，可能是恶意行为或非恶意行为，可能由人为因素或非人为因素（如自然灾害）导致。

就人为因素而言，来自外部的威胁主要是指攻击者利用工控系统的脆弱性，通过病毒（如震网病毒、lesuobingdu）、钓鱼等方式发起攻击（比如持续性威胁APT - Advanced Persistent Threat攻击），渗透进工控系统网络，进行非授权操作或者恶意破坏。攻击者可能包含恶意软件发布者、钓鱼或垃圾邮件发送者、僵尸网络操纵者、犯罪集团等。

来自内部的人为因素威胁主要是指心怀不满的内部员工或者工业间谍，利用工控系统管理或技术方面的缺陷，为恶意报复而删除企业核心数据，或为自身利益窃取企业核心机密售卖给竞争对手。此外，由于工控系统客观存在的脆弱性，人员在访问或操作工控系统时，也可能因为非恶意主观意愿，如误操作，对工控系统造成破坏和影响。

工控系统安全防护

对于上述脆弱性和威胁，企业可通过建立适当的安全防护体系，降低安全风险，以保护工控资产安全和正常生产秩序。普华永道中国建议企业可参考以下五个方面，建立和完善工控安全防护体系：

安全战略与合规

安全战略规划：从企业自身业务战略和IT战略出发，规划工控安全战略与目标；

安全合规：根据企业所在行业和地区，梳理相应监管要求并追踪更新，开展差距分析，整改问题发现，以满足合规要求。

风险评估与管理

资产识别：识别设备设施、硬件、软件、数据、通信协议、文档等工控相关资产，并确定资产价值；

风险识别：识别工控管理层面和技术层面脆弱性，考虑来自内部和外部的威胁；

风险评估：基于所确定的工控资产价值，及识别的脆弱性和威胁，判断风险发生的可能性与影响，对风险进行排序；

风险应对：依据风险评估的结果，规划适当的应对措施，将风险控制在可接受的范围之内。

安全治理与架构

组织架构：建立工控安全管理机构和安全管理负责人，明确并落实安全管理职责，监督安全管理措施的有效运行；

制度与流程：制定工控安全管理制度与流程，包括软硬件管理、身份认证与访问控制管理、数据保护与备份管理、配置与补丁管理、网络与通信管理、设备管理、物理与环境管理、供应链管理、安全审计等；

技术措施：建立全面的工控安全技术架构，包含网络与设备监控、入侵检测与防护、系统配置与更新、边界防护、通信保护、安全域划分、应用安全、数据安全、日志管理、病毒与恶意代码防范、物理与环境安全等；

安全意识：建立工控安全培训机制，提升企业整体安全意识，包括法律法规、企业安全制度与流程、安全事件、安全技术等。

威胁与脆弱性管理

情报收集：持续收集与企业工控系统安全相关的新闻、事件及漏洞等信息，作为安全防护的参考和依据；

漏洞扫描：通过工具，设计扫描窗口期，对工控系统网络内的设备、组件、系统、通信协议等执行扫描，识别工控系统中的漏洞，并对其风险进行评估和排序，采取相应的应对措施；

渗透性测试：通过设计，模拟真实黑客攻击，尝试突破现有安全管控，评估系统抗攻击能力；

通信协议脆弱性分析：通过工具，识别工控系统中的通信协议，分析和评估通信协议的脆弱性。

安全应急管理

应急团队建立：组建应急团队，管理和协调企业工控安全应急工作；

风险场景识别：确定工控安全风险场景，包含数据丢失、设备损坏、通信中断、生产停电、自然灾害等

；

预案建立：依据所确定的风险场景，结合企业实际情况，制定工控安全事件应急预案；

应急演练：针对应急预案开展演练，并根据演练效果更新应急预案。

随着企业业务战略、生产管理模式，以及信息通信技术等方面的不断发展，工控安全防护体系也应随之调整。此外，工业4.0在推动智能制造的同时，也将推动新兴科技应用于现代化生产，包含物联技术、5G、AI、大数据、云计算等。

通讯模块 IC693MDL230 控制卡 调试方便