各工业控制系统用户企业：

随着计算机和网络技术的发展，尤其是信息化和工业化深度融合以及物联网的快速推进，工业控制系统产品广泛采用通用协议、通用硬件和通用软件，越来越多地以各种方式与公共网络连接，病毒、木马等威胁正在向工业控制系统扩散。为了应对工业控制系统信息安全日益严峻的形势，工业和信息化部日前印发《关于加强工业控制系统信息安全管理的通知》（工信部451号文），要求各地区、各有关部门、有关国有大型企业充分认识工业控制系统信息安全的重要性和紧迫性，切实加强工业控制系统信息安全管理，以保障工业生产运行安全、国家经济安全和人民生命财产安全。

为了贯彻落实《通知》精神，了解工业控制系统信息安全现状，工业和信息化部信息安全协调司委托中国电子信息产业集团有限公司第六研究所成立专项课题组，对涉及重点领域的工业控制系统开展信息安全现状调查，研究分析我国工业控制系统信息安全存在问题，并提出相应的措施建议。这是我国第一次开展该类型的调查工作，对于摸清我国工控系统的实际情况，制定有针对性的政策具有非常重要的现实意义，对于我国工控信息安全工作的完善和发展必将产生深远的影响。

课题组联合工业领域各重点行业协会以及《电子技术应用》、《自动化博览》、控制网（www.kongzhi.net）等专业媒体共同开展调查活动，诚邀贵单位参与。课题组郑重承诺，调查数据仅作研究用途，绝不对外泄露，重要研究结论及成果将与被调查企业共享。

中国电子信息产业集团有限公司第六研究所

《我国重点领域工业控制系统信息安全现状调查及问题研究》课题组

2012年2月10日

填 表 说 明

一、 调查范围

本调查表中的主要工控系统是指在核设施、钢铁、有色、化工、石油石化、电力、天然气、先进制造、水利枢纽、环境保护、铁路、城市轨道交通、民航、市政以及其他与国计民生紧密相关的领域中运行的工业控制系统。

二、 填写要求

1、工业控制系统在各行业的应用场景不同而类型不同，填表单位应选择本单位所运营的工业控制系统类型填写，无某类型无需填写;

2、问卷以两种形式提交，请将填写完成的问卷电子版发到：qinyan@ncse.com.cn，同时，请将问卷纸质版加盖单位公章，寄往以下地址：100083，北京市海淀区清华东路 25 号电子六所 秦岩;

3、请尽可能于 2012 年 3 月底之前完成调查问卷的提交;

4、如有任何问题，请联系以下课题组工作人员：

秦岩，电话：010-82306051，Email：qinyan@ncse.com.cn

李林，电话：010-82306008，Email：lilin@ncse.com.cn

工业控制系统信息安全调查问卷

（用户版）

企业名称				单位负责人	
通讯地址	省 市 县（区）			邮政编码	
企业网址				联系电话	
经济类型[1]				所属行业[2]	
填表人		所在部门		职务	
电话		电子邮件		填表时间	

注释:[1]企业经济类型:按国有事业单位、国有及国有控股企业、股份制企业、外商及港澳台投资企业、集体企业、民营企业等填写。

[2]所属行业：按照《国民经济行业分类》（GB/T4754-2011）规定填写。

[3]应用场所、控制对象是指所在分厂、生产车间、所控制的生产工艺加工过程、生产机械与装备。

[4]信息安全防护：产品中采用的信息安全技术与系统中集成的信息安全相关产品分别填写，可参考备注中的内容填写编号，备注中没有的内容请用文字填写。

1、企业主要工控系统应用基本情况

主要工控系统	数据采集监控系统(SCADA)	分布式控制系统(DCS/FCS)	工业 PC 机(IPC)	数控系统(CNC)
安装数量、投资情况	目前总数_____台套 总投资_____万元 2015 年预计_____台套 总投资_____万元	目前总数_____台套 总投资_____万元 2015 年预计_____台套 总投资_____万元	目前总数_____台套 总投资_____万元 2015 年预计_____台套 总投资_____万元	目前总数_____台套 总投资_____万元 2015 年预计_____台套 总投资_____万元
产品来源（国产品牌）	供应商名称 1、_____ 数量：_____台套 2、_____ 数量：_____台套 3、_____ 数量：_____台套	供应商名称 1、_____ 数量：_____台套 2、_____ 数量：_____台套 3、_____ 数量：_____台套	供应商名称 1、_____ 数量：_____台套 2、_____ 数量：_____台套 3、_____ 数量：_____台套	供应商名称 1、_____ 数量：_____台套 2、_____ 数量：_____台套 3、_____ 数量：_____台套
产品来源(国外品牌)	供应商名称 1、_____ 数量：_____台套 2、_____ 数量：_____台套 3、_____ 数量：_____台套	供应商名称 1、_____ 数量：_____台套 2、_____ 数量：_____台套 3、_____ 数量：_____台套	供应商名称 1、_____ 数量：_____台套 2、_____ 数量：_____台套 3、_____ 数量：_____台套	供应商名称 1、_____ 数量：_____台套 2、_____ 数量：_____台套 3、_____ 数量：_____台套
应用场所、控制对象[3]				
组网情况	□ 不可联网 □ 接入控制系统内部网络 □ 无线接入 □ 与管理信息系统连接 □ 连入企业信息网 □ 其它：_____	□ 不可联网 □ 接入控制系统内部网络 □ 无线接入 □ 与管理信息系统连接 □ 连入企业信息网 □ 其它：_____	□ 不可联网 □ 接入控制系统内部网络 □ 无线接入 □ 与管理信息系统连接 □ 连入企业信息网 □ 其它：_____	□ 不可联网 □ 接入控制系统内部网络 □ 无线接入 □ 与管理信息系统连接 □ 连入企业信息网 □ 其它：_____
信息安全防护[4]	系统中采用的信息安全防护技术 硬件：_____ 软件：_____ 其它：_____	系统中采用的信息安全防护技术 硬件：_____ 软件：_____ 其它：_____	系统中采用的信息安全防护技术 硬件：_____ 软件：_____ 其它：_____	系统中采用的信息安全防护技术 硬件：_____ 软件：_____ 其它：_____
	系统中集成的信息安全产品 1、_____ 2、_____	系统中集成的信息安全产品 1、_____ 2、_____	系统中集成的信息安全产品 1、_____ 2、_____	系统中集成的信息安全产品 1、_____ 2、_____
	备注：可参考以下信息安全防护机制、技术及产品填写： ①专用操作系统、专用数据库 ②接入控制和身份鉴别 ③内容过滤 ④数据加密、VPN ⑤安全审计、漏洞扫描 ⑥防恶意软件(含病毒、蠕虫等) ⑦防火墙、防水墙与入侵检测 ⑧网络隔离 ⑨容灾备份			
	信息安全防护存在的问题:			
信息安全责任约定	是否已在供货合同中或以其他方式明确供应商应承担的信息安全责任和义务？ □ 是，主要内容包括：_____。 □ 否			

1、企业主要工控系统产品基本情况（续）

主要工控系统	PLC 可编程序控制器	工业机器人	数字调节器	其他
安装数量、投资情况	目前总数_____台套 总投资_____万元 2015 年预计_____台套 总投资_____万元	目前总数_____台套 总投资_____万元 2015 年预计_____台套 总投资_____万元	目前总数_____台套 总投资_____万元 2015 年预计_____台套 总投资_____万元	目前总数_____台套 总投资_____万元 2015 年预计_____台套 总投资_____万元
产品来源（国产品牌）	供应商名称 1、_____ 数量：_____台套 2、_____ 数量：_____台套 3、_____ 数量：_____台套	供应商名称 1、_____ 数量：_____台套 2、_____ 数量：_____台套 3、_____ 数量：_____台套	供应商名称 1、_____ 数量：_____台套 2、_____ 数量：_____台套 3、_____ 数量：_____台套	供应商名称 1、_____ 数量：_____台套 2、_____ 数量：_____台套 3、_____ 数量：_____台套
产品来源(国外品牌)	供应商名称 1、_____ 数量：_____台套 2、_____ 数量：_____台套 3、_____ 数量：_____台套	供应商名称 1、_____ 数量：_____台套 2、_____ 数量：_____台套 3、_____ 数量：_____台套	供应商名称 1、_____ 数量：_____台套 2、_____ 数量：_____台套 3、_____ 数量：_____台套	供应商名称 1、_____ 数量：_____台套 2、_____ 数量：_____台套 3、_____ 数量：_____台套
应用场所、控制对象				
组网情况	□ 不可联网 □ 接入控制系统内部网络 □ 无线接入 □ 与管理信息系统连接 □ 连入企业信息网 □ 其它：_____	□ 不可联网 □ 接入控制系统内部网络 □ 无线接入 □ 与管理信息系统连接 □ 连入企业信息网 □ 其它：_____	□ 不可联网 □ 接入控制系统内部网络 □ 无线接入 □ 与管理信息系统连接 □ 连入企业信息网 □ 其它：_____	□ 不可联网 □ 接入控制系统内部网络 □ 无线接入 □ 与管理信息系统连接 □ 连入企业信息网 □ 其它：_____
信息安全防护[4]	系统中采用的信息安全防护技术 硬件：_____ 软件：_____ 其它：_____	系统中采用的信息安全防护技术 硬件：_____ 软件：_____ 其它：_____	系统中采用的信息安全防护技术 硬件：_____ 软件：_____ 其它：_____	系统中采用的信息安全防护技术 硬件：_____ 软件：_____ 其它：_____
	系统中集成的信息安全产品 1、_____ 2、_____	系统中集成的信息安全产品 1、_____ 2、_____	系统中集成的信息安全产品 1、_____ 2、_____	系统中集成的信息安全产品 1、_____ 2、_____
	备注：可参考以下信息安全防护机制、技术及产品填写： ①专用操作系统、专用数据库 ②接入控制和身份鉴别 ③内容过滤 ④数据加密、VPN ⑤安全审计、漏洞扫描 ⑥防恶意软件(含病毒、蠕虫等) ⑦防火墙、防水墙与入侵检测 ⑧网络隔离 ⑨容灾备份			
	信息安全防护存在的问题:			
信息安全责任约定	是否已在供货合同中或以其他方式明确供应商应承担的信息安全责任和义务？ □ 是，主要内容包括：_____。 □ 否			

2、近年来产品在用户使用过程中存在信息安全问题及事故情况

系统名称	发现问题的工控系统 1	发现问题的工控系统 2	发现问题的工控系统 3
主要问题	☐ 感染恶意软件(类型：____，____，____) ☐ 外部攻击 ☐ 内部人员有意破坏 ☐ 线路中断 ☐系统安全缺陷 ☐ 软硬件配置安全级别低 ☐ 其它： _________	☐ 感染恶意软件(类型：____，____，____) ☐ 外部攻击 ☐ 内部人员有意破坏 ☐ 线路中断 ☐系统安全缺陷 ☐ 软硬件配置安全级别低 ☐ 其它： _________	☐ 感染恶意软件(类型：____，____，____) ☐ 外部攻击 ☐ 内部人员有意破坏 ☐ 线路中断 ☐系统安全缺陷 ☐ 软硬件配置安全级别低 ☐ 其它： _________
如何发现	☐ 工作人员监测、分析 ☐ 通过安全产品发现 ☐ 意外发现 ☐ 有关部门通知或他人告知 ☐ 其它：_________	☐ 工作人员监测、分析 ☐ 通过安全产品发现 ☐ 意外发现 ☐ 有关部门通知或他人告知 ☐ 其它：_________	☐ 工作人员监测、分析 ☐ 通过安全产品发现 ☐ 意外发现 ☐ 有关部门通知或他人告知 ☐ 其它：_________
造成损失	☐ 设备损坏 ☐ 数据损失 ☐ 人员伤亡 ☐ 环境污染 ☐ 经济损失，数额：_________ ☐ 业务中断 ☐ 其它： _______	☐ 设备损坏 ☐ 数据损失 ☐ 人员伤亡 ☐ 环境污染 ☐ 经济损失，数额：_________ ☐ 业务中断 ☐ 其它： _______	☐ 设备损坏 ☐ 数据损失 ☐ 人员伤亡 ☐ 环境污染 ☐ 经济损失，数额：_________ ☐ 业务中断 ☐ 其它： _______

注：信息安全问题及事故情况，请如实填写，仅作数据分析使用，绝不外泄，也不作为任何追责依据。

3、企业工控系统的信息安全防护情况

企业工业控制系统采取了哪些信息安全防护手段（可多选）
☐ 企业关键工业控制系统与企业信息系统之间存在隔离机制 ☐ 定期进行工业控制系统的连接检查 ☐ 对工业控制系统的所有外部连接进行登记备案 ☐ 对工业控制系统的所有外部连接定期进行风险评估 ☐ 定期检查工业控制系统的配置的安全性 ☐ 及时升级信息安全防护产品 ☐ 针对可能发生的信息安全事件制定有应急预案 ☐ 制定并严格执行人员管理安全措施 ☐ 定期对员工进行信息安全培训
企业对工控系统信息安全性的看法与计划
（1）企业希望政府制定哪些优惠政策以支持工控信息安全工作？ ☐ 税收减免 ☐ 专项资金支持 ☐ 准入制度 ☐ 其它：________________________ （2）如何制定并推广工业控制系统信息安全标准、规范？ ☐ 政府主导 ☐ 龙头企业主导 ☐ 行业协会主导 ☐ 本企业愿意参加制定相关标准规范 ☐ 其它：________________________ （3）是否有必要建立工业控制系统风险评估制度？ ☐ 是，原因：__________________________________ ☐ 否，原因：_________________________________ （4）是否有必要建立工业控制系统产品入网安全检测及论证制度？☐ 是 ☐ 否
其他技术、管理措施建议及计划
（1）设立信息安全管理机构

（2）采用信息安全产品

（3）对数据采取加密措施

（4）建立工控系统信息安全定期测评制度

（5）其他技术、管理措施