# 工控系统网络安全防护探讨

曹 湛

（中国航发沈阳发动机研究所，辽宁 沈阳 110000）

**摘 要** 工控系统彰显着计算机先进技术的存在价值，工控技术以及计算机技术和通讯技术打造了完整的工控系统。本文主要以工控系统网络的安全防护为重点进行阐述，首先分析工控系统网络的防护影响因素，其次从增强工控系统用户安全防护水平，明确安全防护意识、划分网络安全界限，强化软件安全保障、创新安全防护技术，推动工控系统的安全建设几个方面深入说明并探讨安全防护措施，目的是给相关研究提供参考。

**关键词** 工控系统网络；安全防护；体系构建

**中图分类号**：TP393.08 **文献标识码**：A **文章编号**：1007-0745(2023)01-0022-03

如今，网络已经深深存在于各行各业，在工业生产管理中引进网络技术，创设比较完整的工业控制体系是必然趋势。工业控制充当工业技术持续化创新的基本要点，更是工业朝向现代化发展的条件，对工业行业的经营和管理起到重要作用。工控系统网络中，安全防护是比较关键的项目，然而具体的安全防护中面临着些许问题，值得相关人员具体研究。

## 1 工控系统网络的防护影响因素

工控系统以得到真实化信息为基础，以传感器的方式得到数据保存在计算机内，后续通过计算机给予相关的信息数据加以动态分析和处理。在工控系统的支持下，不仅实现了自动化数据处理的目的，还提高了计算的正确率。工控系统有传感器模块、发射器模块与转换器模块等，传感器能够合理监督物品的物理参数，加快计算机的运行速度[1]。转换器能够把数据转变为电信号，之后以电信号的形式保存在计算机内。发射器能够控制电信号朝终端方向运输，综合来看最为关键的模块是控制器，提高了数据信息的准确性。另外，工控系统之内的电信号输入过程与电信号输出过程都是建立在控制器全方位运作基础之上，系统在控制器的运作中贯彻电信号的复原项目。

研究工控系统网络的安全防护影响因素：

第一点是工控系统自身的因素，此系统具备较强的综合性与繁琐性，应用的范围比较广。因此在具体设计上和运作中对工作者提出更加严格的条件，系统自身与操作流程都是潜在网络安全隐患的。

第二点是网络风险的出现，工控系统的运作期间，网络化运用是比较关键的趋势，每一个领域之内发挥工控系统功能时，应重视数据采集、数据研究与数据管理，工控系统以及网络系统被远程操控。在此阶段，工控系统的一些结构可能存在于公共网络之内，可是公共网络的环境时刻面临着网络信息的安全隐患威胁，因此工控系统可能在病毒与黑客等条件制约之下出现安全问题。以“百度百科”为例，借助引擎模块开展Open Directory的信息搜索，会得到较多和工控系统存在关系的数据，若黑客入侵以及人为攻击，势必影响网站体系的管理质量[2]。

第三点是工业控制标准接口有着协议漏洞的情况，工控系统的运作中，相关网络结构是借助“以太网”加以创设，那么在一定环境中工业控制标准接口可能是具备显著开放性的，操作这一个系统，由于控制标准的信息获取与接口传输缺乏了信息保护的过程，再这工业控制标准的协议和其他类型代码均潜在漏洞，同时漏洞是在外界风险干扰下产生的，这样便凸显控制接口的协议漏洞。

第四点是工控体系比较脆弱，我国一些工控系统在运作中，均体现出内部结构的不足，这样工控系统很容易面临脆弱性威胁，特别是网络资源的配置与硬件设定以及边界问题，使得工控系统的网络面临安全风险，造成工控系统的安全问题出现。

## 2 工控系统网络的安全防护措施

### 2.1 增强工控系统用户安全防护水平，明确安全防护意识

首先，形成一定的工控系统网络安全防护思路，安全思路是工控系统网络安全防护的前提条件，为工控系统的安全防护提供了指导，工作者要关注工控系

统的脆弱问题，把以往网络安全管理的有效经验作为基础，加强网络安全措施的创新，使得工控系统的网络运作可以足够安全和规范。比如实施补丁操作，关联工控系统的创新条件，相关人员要补丁转型工控系统的结构体系，避免工控系统处于公共环境中有漏洞风险[3]。工作者应重视测试检验，给工控系统的安全运作提供真实化环境，多次检验和评价实施工控系统的备份加工，确保补丁可以全方位转型，控制具体升级以及转型阶段面临的风险。之后是实施工控系统的隔离方案搭建，隔离方案的拟定可直接控制工控系统的运作出现风险，工作者需要深层次研究工控系统的防护目标，明确隔离方案与计划，科学应用以及实践。一般而言，工控系统的工作者要结合不相同领域的体系运作条件，优化仪器设备的性能，围绕优化内容开展针对性调试操作，使得多个结构体系能够规范运作，降低设备之间衔接不够时效的概率。基于工控系统的安全防护关键点，即划分隔离防护的模块，尤其是内网模块、外部模块、操作模块与隔离模块，利用规范化举措加以针对性改善，贯彻风险管理工作。

其次，形成物理模式的防护机制，根据相关资料可以明确，对工控系统加以物理层面的机制搭建，能够彰显工控系统管理的安全性与可行性，还是工控系统安全建设的前提项目，决定着工控系统作用的发挥[4]。因此，相关人员实施工控系统的整合设计时，应以物理视角处理工控系统的安全风险，可实施门禁机制，避免其他人员走进工控的现场，结合企业的基本理念构建对应先进生产设备梦，包含备用发电机、备用电线以及备用工具，降低生产问题的出现率。这样配置监督管理计划，可实现工控系统的一体化安全监督工作，及时了解问题和处理问题，挖掘内在的风险因素与生产因素，逐步使得工控系统的运作效率得以提升。

最后，对网络渗透的现象进行优化，工作者应重视网络渗透情况的出现，以换位研究的模式对设计完成的工控系统安全结构进行检验，从多个视角分析安全防护的基本对策，真正做好工控系统的安全防护项目，增强工控系统用户的安全防护水平。

### 2.2 基于网络安全需求，完善工控系统的三层架构

和以往的信息系统相比较，工控系统网络安全防护应具备特殊性。首先，存在边界防护的问题，网络安全边界防护会对工控系统的安全保障产生一定的影响，然而目前的工控系统尚未真正落实边界防护思路，即边界防护没能和具体的标准相匹配，引出工控系统的多个业务项目潜在安全风险。

其次，存在远程访问的问题，实施工控系统的远程维护作为关键的维护操作，可是对应远程维护的通道均是以供应商为主提供的，若不能完善远程访问防护结构，是会在维护期间产生恶意入侵风险的[5]。

再次，存在监督需求以及审计问题。工控系统的具体生产，相关人员要细致地进行监督方案的设置与审计方案的设置，此工作包含网络监督等软件，一些生产厂家未对设备进行数据监督，无形中埋下了安全隐患，所以应强调审计检验，控制工控系统的网络安全问题。

最后，是漏洞管理与风险防范的问题，工控系统的网络安全防护上，经常使用的系统是微软，因为控制网络提出了工控系统结构的较多要求，可能增加系统漏洞的筛查难度和升级难度，使得操作系统整体上面临安全隐患。工控系统的管理工程中，需安设对应杀毒软件以提高网络运作安全性，可是在没能及时安装先进软件的前提下是会出现恶意代码攻击破坏网络的，阻碍工控系统的高效率运作，因此风险防范也是应该及时进行的，为工控系统网络安全防护奠定基础[6]。

除此之外，要想真正实现工控系统的网络安全防护，应制定三层结构框架，第一层是计划管理，即工作者以工作计划为前提进行高效率工作，一般来讲计划管理的负责人应使用管理服务器。第二层是制造管理，此层和计划管理存在着相同点，也就是共同和服务器衔接，制造管理的设定还要额外构建计算机系统，体现制造管理的专业性。第三层是工业控制，其作为比较繁琐的模块，一方面应该和服务器与终端互相衔接，另一方面应及时呈现访问记录。第一层以及第二层的设定，贯彻了实名制的思路，使得网络运作更加具备安全性，增强网络保障的综合效果。全方位监督网络信息数据，最大化避免软件代码攻击到工控系统，让工控系统的网络管理面临威胁，落实工控系统的各层工作项目。基于此进行工控系统的网络安全防护，对各个层级的任务进行分配，更好地避免了工控系统的网络安全问题出现，有利于保障工控系统的综合性能。

### 2.3 划分网络安全界限，强化软件安全保障

对于工控系统的网络安全防护过程，要基于安全隐患进行针对性模块划分，以风险为主，按照不同防护要求实施工控系统的网络安全保护。特别是网络控制与数据网络的内在数据传输，加密化处理信息通道，

赋予工控系统的内部网络管理较强稳定化特征。信息网以及外部管控网的衔接上，还需要配置对应加密，内部网络以及数据网之间适当配置安全过滤装置，避免网络攻击到工控系统的现象出现。利用数据网确定数据应用的范围，控制工控系统安全隐患，精准化落实工控系统的安全防护工作[7]。在软件安全保障上，工控系统的体系完善不仅应体现硬件的作用，还应体现软件的防护，针对公共体系内的一些软件，工作者要按照定期杀毒的思路优化设备性能，尤其是安设防火墙。对溶液内设计图纸的数据信息进行加密化管理，排除由于工控系统软件防护问题所致的网络问题，定时优化工控系统的操作流程，对操作设备进行整体更新，能够兼容的条件下整合系统结构，这样可以减少操作漏洞的出现，更好地保障了软件运作安全。

2.4 创新安全防护技术，推动工控系统的安全建设

具体的工控系统网络安全防护中，部分先进技术的应用可以起到积极作用。首先是代码防护技术，以往的网络保障中以黑名单病毒查杀的形式进行，可是不可规避出现错误删除的现象，此种模式针对一般形式的系统而言带来较大程度的伤害。安全防护上，可选取白名单进行病毒查杀的问题，显著提高病毒查杀效果，避免产生信息错误删除的情况。

其次是主机外设技术，一些工作者把手机等关键设备和系统主机进行连接，可能出现木马病毒，不利于保障工控系统运作的安全性，所以健全工控系统的主机外设管理机制十分关键。

最后是漏洞挖掘技术，利用此种技术直接定位漏洞的范围，最大化研究漏洞的恶化趋势，探索行之有效的措施挖掘内在漏洞，安排专业能力比较强的工作者全方位研究，一旦出现问题应即刻处理，避免漏洞给工控系统的网络安全带来威胁[8]。

需要注意的是，工控系统的网络安全防护中，性能比较重要的设备也是要被隔离化加工的，第一个是工业隔离模式，工控系统的结构之中，以隔离的思路处理孔子体系，一方面提高工控系统的信息采集及时性，另一方面控制工控系统安全风险产生，落实网关与物理格局处理等关键任务。第二个是“2+1”隔离，即对工控系统之中的控制模块与数采机模块进行隔离，此种隔离结束后不输入私密密码是不能使用控制系统的，由此全面对工控系统的安全系数进行提升。在隔离化加工之后，工控系统的网络安全风险会有所降低，提高工控系统网络安全防护的现代化发展速度。

## 3 结语

综上所述，工控系统的生产组织，充当工控系统的执行者与生产者，要充分关注网络安全设计，即在具体生产阶段强化工控系统的水平。此系统的生产机构要大力开发技术，利用先进的技术完善工控系统的体系，确保工控系统可以在时代变化之下不断发展，体现工控系统搭建的完整性，巧妙避免工控系统的内在风险出现。并且促进工控系统的网络安全防护，由于工控系统已经存在于各个行业，对应地位是比较重要的，不管是安全保障还是稳定保障，都影响到社会的发展。政府和第三方单位需要实施自我职能，提高工控系统安全防护的速度，明确规范化的网络安全机制，不要因为网络而产生恶意破坏的现象，利用网络安全防护标准，从根源上对工控系统等一系列设施的综合性进行研究，真正保障自我权益。

**参考文献：**

[1] 王子洋，何文．大型石化控制系统替换升级过程中网络安全防护策略设计[J]．自动化与仪表，2021,36(09):34-39.

[2] 张悦，荆琛，衣然．基于等保2.0的重点行业工控系统网络安全防护策略研究[J]．信息技术与网络安全，2021,40(09):54-57,76.

[3] 叶鑫豪，周纯杰，朱美潘，等．DDoS攻击下基于SDN的工业控制系统边云协同信息安全防护方法[J]．信息安全研究，2021,07(09):861-870.

[4] 顾志华，楼立，王小栋，等．自动化码头岸边集装箱起重机工控系统信息网络安全防护设计[J]．港口装卸，2021(04):24-26.

[5] 李朋，韩辛酉，李焕．油气田企业工业控制系统网络安全风险与对策分析[J]．信息系统工程，2021(08):107-109.

[6] 刘刚，林棋，边学文．工业控制网络安全性分析——以中亚某天然气管道为例[J]．石油工业技术监督，2021,37(08):29-32.

[7] 张琴玲，侯正炜，桂华．火电厂工业控制系统网络安全等级保护设计研究[J]．智能物联技术，2021,04(04):22-28.

[8] 唐嘉，赵咏，韩涛．某石油化工企业基于等保2.0的工控系统网络安全评估与建议[J]．网络安全和信息化，2021(07):127-129.