工业安全网关产品白皮书

■ **文档编号**	NSF-PROD-ISG-V2.0-产品白皮书-V1.1	■ **密级**	完全公开
■ **版本编号**	V1.1	■ **日期**	2018-10-25

■ **版本变更记录**

时间	版本	说明	修改人
2018.02.11	V1.0	初版	
2018.10.25	V1.1	调整内容结构，增加部分内容	

■ **适用性声明**

本模板用于撰写绿盟科技内外各种正式文件，包括技术手册、标书、白皮书、会议通知、公司制度等文档使用。

目录

表格索引

未找到目录项。

插图索引

未找到目录项。

一. 产品概述

1.1 行业背景

随着网络信息时代的到来，我国工业模式发生了翻天覆地的变化，彻底打破了“信息孤岛”模式，企业全面联网，生产数据轻松实现汇总分析，不但提高了生产效率，还达到了节能减排的目的。信息化给工业带来的有利变化显而易见，但随之而来的网络安全问题又使人为之担忧。

在工业网络中，运行着 DCS、PLC、SCADA 等各种过程控制系统，它们往往是生产系统的核心，负责完成基本的生产控制和监控。这些过程控制系统一旦遭受干扰或破坏，就会对工业生产造成不同程度的影响，可能使企业蒙受重大的经济损失，危及生产人员的生命安全，甚至造成重大社会危害。近年来发生的工业网络入侵事件给我们敲响了警钟，如何高正过程控制系统的运行安全迫在眉睫，，广大工业企业迫切需要一款针对工业网络进行有效安全防护的专业网关产品。

1.2 工业控制系统网络环境特点

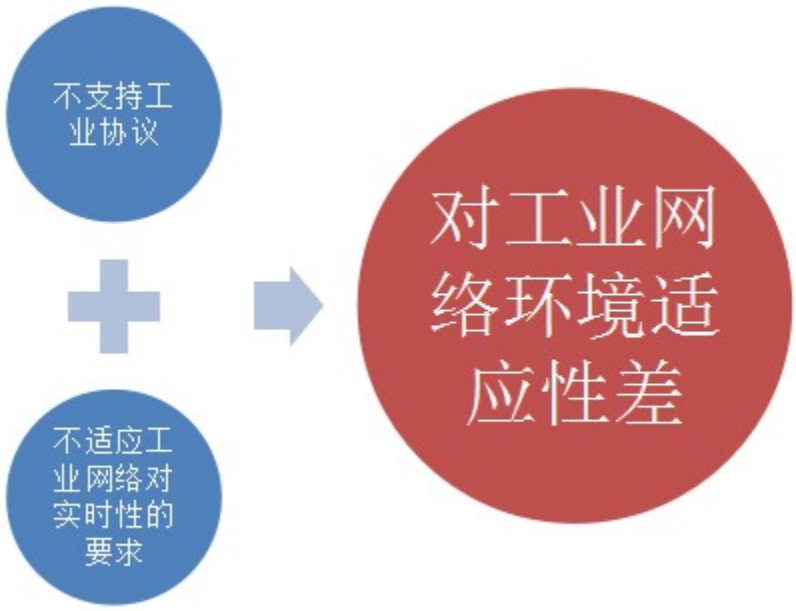
工业控制系统网络是由工业自动化生产设备，如 SCADA、DCS、PLC 等各种过程控制系统组成的网络，不同于 IT 网络，工业控制系统网络具有以下特点：

- 专用通信协议或规约（OPC、Modbus、DNP3 等）；
- 系统传输、处理信息的实时性要求高，尽量避免停机、重启等操作；
- 系统故障必须及时响应处理，不可预料的中断会造成经济损失或其他危害；
- 为满足特定应用场景、任务单一性以及系统稳定性；同时为保障生产的连续性，减少可能的风险，系统或设备很少升级，甚至不升级。

1.3 传统防火墙在工业控制系统网络中应用的不足

传统防火墙是目前网络边界上最常用的一种防护设备，诞生于传统信息网络环境下，虽然经过了多年的发展和完善，但其应用环境还是局限于企业信息网络，它对于工业网络环境还有诸多的不适应。

- 传统防火墙主要是针对通用网络协议进行审核和防护，不能对工业网络协议和应用数据的内容进行解析和检查；
- 传统防火墙基于黑名单机制，为及时应对新发现的系统和软件漏洞，以及面临不断更新的网络攻击手段和威胁需要不断升级，不符合工业现场的特点。



1.4 ISG 系列工业安全网关产品简介

绿盟科技 ISG 系列工业安全网关不但支持传统防火墙的基础访问控制功能，重要的是它提供针对工业协议的指令级深度检测，实现了对 Modbus、OPC DA、DNP3 等主流工业协议和规约的细粒度检查和过滤，帮助用户防护来自网络的病毒传播、黑客攻击等行为，避免其对控制网络的影响和对生产流程的破坏，同时具备 Bypass 及全透明无间断部署功能，保证业务的连续性；规则报警功能可以有效的对异常操作进行处理，避免

因未及时处理造成损失和危害；而且它采用白名单机制，可以较少甚至不用升级，符合工业现场特点。

二. 产品架构

ISG 系列工业安全网关产品在架构设计上充分的考虑了工业网络设备种类多、协议复杂、行业差别大的特点，将产品进行了深度的模块化封装，引入了功能插件的概念，使整个防火墙系统更加部件化。通过这种架构的实现一方面可以更好的适应现有工业网络安全防护的需要，另一方面为未来产品功能的扩展和用户定制开发打下良好的基础。

ISG 系列工业安全网关包括基础系统、业务模块和配置管理三个部分：

- 基础系统是由绿盟科技根据工业网络通信特点和安全防护要求定制开发的底层运行平台，为防火墙上层业务模块提供必要的运行环境和安全保障；

- 业务模块是 ISG 系列工业安全网关的核心业务处单元，主要用于完成对于工业网络协议的识别、解析、深度过滤和攻击防护；
- 配置管理采用 B/S 架构，用于对 ISG 系列工业安全网关进行策略配置和运行监控，是与安全网关进行人机交互的接口。

三. 产品功能特点

ISG 系列工业安全网关具有安全性、可用性及可靠性三大功能特点。

3.1 安全性

3.1.1 工业网络通信协议深度包检测

传统防火墙主要是针对通用网络协议进行访问控制和安全过滤，完全不支持工业通讯协议。ISG 系列工业安全网关与传统防火墙最大的区别是针对工业通讯协议进行深度包检测。之所以称之为深度过滤，是因为 ISG 系列工业安全网关不但可以针对工业网络协议进行基本的访问控制，而且可以针对工业网络协议的内容和数据进行细致的合规性检查，例如：ISG 系列工业安全网关的 Modbus 协议规则可以针对 Modbus 协议的设备地址、寄存器类型、寄存器范围和读写属性等进行检查，能有效的防范各种非法的操作和数据进入现场控制网络，最大限度地保护控制系统的安全。

工业现场设备繁多、规格不一、通信协议和规约各异，这就要求安全设备可以支持多种工业网络通信协议、适用于各种网络环境、可与各种现场设备进行交互对接。针对这种现状 ISG 系列工业安全网关将每一个工业协议作为一个独立的深度过滤单元，根据不同协议进行设置。而且可以根据用户现场的需要进行工业网络协议深度过滤的快速定制开发和响应，最大限度的满足工业现场的各种安全防护要求。当遇到不支持的特有协议，绿盟科技具备专业的开发团队，可根据客户需求进行定制开发。

3.1.2 通用网络协议防护

ISG 系列工业安全网关可对通用网络协议进行访问控制和安全过滤，具有 4-7 层包过滤,支持以五元组形式对通用协议数据包进行访问控制和安全过滤。能够支持常见的网络协议（如 TCP、UDP、HTTP、HTTPS、ICMP、FTP、TELNET、视频协议、数据库等）且对 HTTP、FTP、TELNET 等协议具有深度及粒度的深度过滤功能，支持网站安全浏览、邮件访问控制、FTP 访问控制、数据库访问控制、文件同步等安全规则。同时也支持基于 IP/MAC 绑定的安全策略设置，使伪造 IP 的数据包无法通过工业安全网关。

3.1.3 安全攻击防护

ISG 系列工业防火墙具有以下攻击防护：

- Dos/DDos 攻击防护：其中包括 TCP Flood 攻击、UDP Flood 攻击、SYN Flood 攻击、ICMP Flood 攻击、IP Flood 攻击、TCP 最大连接数等；
- 异常数据包攻击防护：其中包括 Ping of Death 攻击、TCP 碎片攻击、IP 碎片攻击、LAND 攻击等；
- 扫描防护：对 SCANPORT 攻击进行防护。

3.2 可用性

3.2.1 全透明、不间断部署

考虑到工业网络对于可用性、持续性的要求，ISG 系列工业安全网关采用全透明接入的方式，提供直通、测试、管控三种工作模式，产品在部署、配置和使用过程中可以根据需要实时切换到适当的工作模式下，保证在整个部署过程中都不会阻断正常的业务数据传输，无需中断生产系统的运行，同时在启动深度过滤时可选择仅警告，等确认后再进行处理，保障生产系统不间断运行。

- 直通模式：开启直通模式，ISG 系列工业安全网关可允许所有数据包直接传输，所设定的规则不生效，且不产生日志；
- 测试模式：开启测试模式，ISG 系列工业安全网关可允许所有数据包直接传输，但会对每个数据包进行分析，验证所设置的安全规则，并生成日志，方便用户验证自己的规则是否有误或遗漏；
- 管控模式：开启管控模式，ISG 系列工业安全网关会按照所设定的规则进行运行，不符合规则的将被禁止通过，符合规则的则通过，并生成日志。

3.2.2 智能协议识别和辅助规则生成

工业网络中设备众多、网络通信复杂，用户很难全面的掌握网络中所必须的业务通信需求，这会给防火墙的规则配置带来很大的困难。为了方便用户进行防火墙规则的配置，提高规则配置的准确性，减少规则配置的工作量，ISG 系列工业安全网关具备智能协议识别和辅助规则生成功能。

智能协议识别功能采用被动检测的方式从网络中采集数据包，并进行数据包的解析，智能的与系统内置的协议特征、设备对象等进行匹配，生成可供参考的网络交互信息列表，帮助用户以最快捷的方式了解和掌握网络中的业务通信。

用户可以在测试模式下使用策略管理的辅助配置功能生成辅助规则，将网络交互信息与实际业务进行比对，给每一个网络交互过程配置适当的防护规则，从而准确、快捷的完成防护规则的部署。

3.2.3 日志管理

ISG 系列工业安全网关支持多个 Syslog 日志服务器，可产生不同级别、类型的日志，并对日志进行管理配置，具有日志审计功能，可以根据不同条件进行日志查询等操作。

3.2.4 实时流量监控

ISG 系列工业安全网关可以对各个网口流量以秒为单位进行流量的实时统计。

3.2.5 简便的配置方法

ISG 系列工业安全网关采用 B/S 架构，通过浏览器直接对防火墙进行配置，无需安装应用软件，配置过程简单，容易上手。ISG 系列工业安全网关配置具有以下几个特点：

- **“白名单”配置方式**

ISG 系列工业安全网关默认拒绝所有连接，用户只需要根据工业现场实际的业务通信需要配置与业务相关的放行规则即可，无需关心不需要的网络通信协议。

- **内置各种常用协议**

ISG 系列工业安全网关内置了常用工业网络协议、通用网络协议等协议对象，在进行防火墙配置时可以直接引用即可。

3.3 可靠性

3.3.1 硬件可靠性保障

为了适应工业网络环境对于产品可靠性的要求，ISG 系列工业安全网关采用工业级产品硬件设计，在环境适应性、散热、故障处理等方面进行了全面的优化。

- 硬件平台专门面向工业应用场合设计，对 PCB、电源、机箱结构、散热进行全面优化，采用低功耗、宽温、宽压电子元器件，多种模式的导散热方式，充分的减少产品的发热量，提高产品的稳定性和环境适应性，保证设备在各种恶劣环境下可以持续、稳定的运行；

- 网口支持 Bypass 功能，根据系统运行状态开启，也就是系统断电、关机及启动过程中开启；
- 具有硬件狗功能；
- 具备双机热备功能(ISG NX3-1000A 不支持)。

3.3.2 软件可靠性保障

为了符合工业现场生产的连续性及稳定性，ISG 系列工业安全网关在软件上进行全面优化设计：

- 系统内嵌自诊断程序，实时监测系统的运行情况，支持系统故障自恢复功能；
- 具有全透明无间断部署功能，保证系统运行稳定性和不间断性；
- 具有智能协议识别和辅助规则生成方便用户进行协议规则配置；
- 具有软件狗、工程备份、流量限制、日志审计等功能。

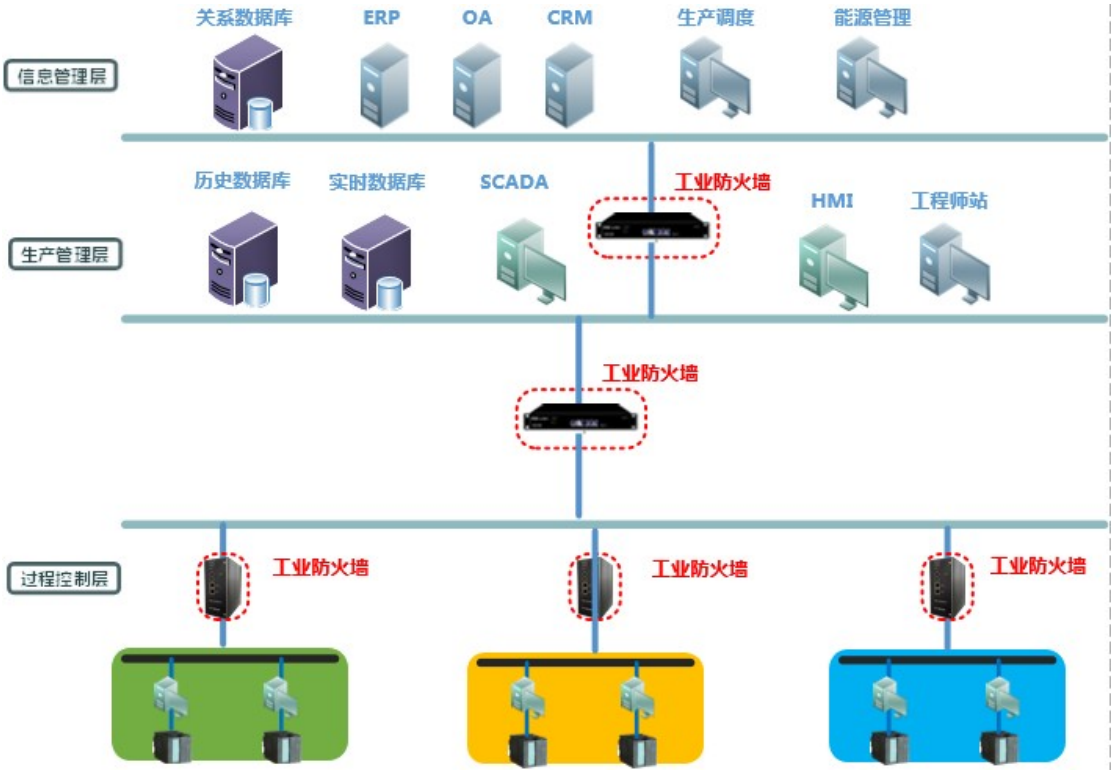
四. 典型应用

4.1 安全区域之间的访问控制和安全防护

随着“两化融合”的不断推进，广大工业用户的网络结构发生了重大变化，现场过程控制网络、生产管理网络、企业信息网络正被打通，网络纵向分层、横向分区的模式正在形成。由于各个层次、各个区域网络的业务不同、作用不同，对于安全防护的要求也就不同，所以需要在不同安全区域之间进行必要的防护和控制。ISG 系列工业安全网关可以帮助用户很好的实现这一目标。

首先通过在纵向不同层次网络之间部署 ISG 系列工业安全网关，并配置合理的访问规则，可以控制不必要的跨层访问，防止攻击者通过上层网络向下层网络的渗透和攻击，减少由于网络互联互通所带来的安全风险。同时可以对不同层次之间的工业协议数据交换进行深度过滤，屏蔽非法操作，保障生产安全。

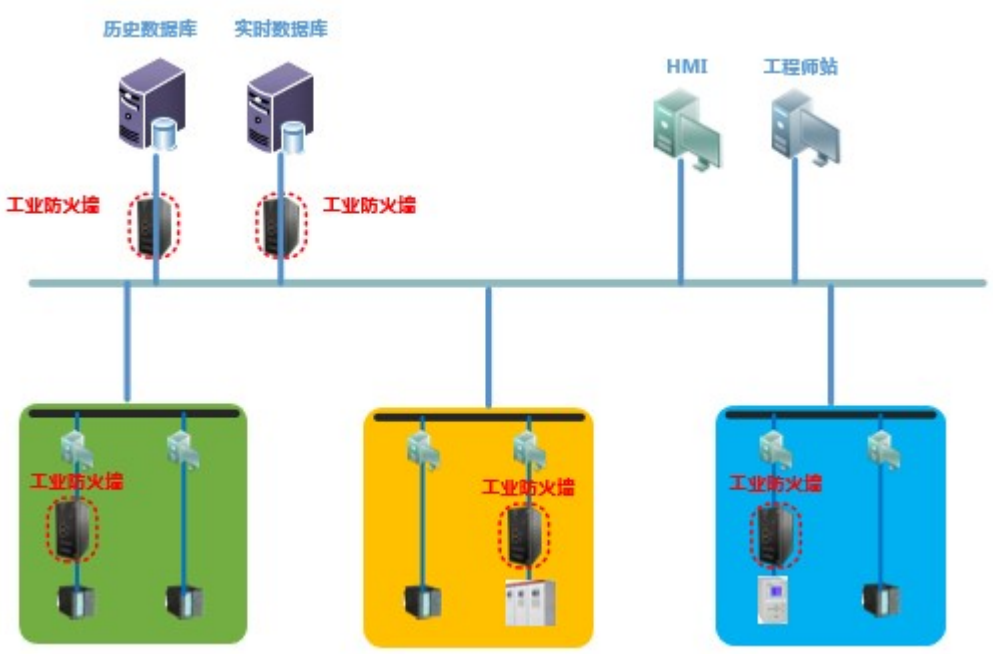
其次还可以在同一网络层次中平行的厂区、工艺流程和业务子系统之间部署 ISG 系列工业安全网关，将它们分割成不同的安全区域，配置不同的访问规则，屏蔽不同安全区域之间不必要的访问，对不同安全区域之间的工业协议数据交换进行深度过滤，减少安全区域之间安全问题的扩散和影响。



4.2 重点设备的安全防护

在工业网络中存在很多核心的控制器、重要的数据存储和交换服务器，它们是整个工艺流程和生产过程的中枢，关系到生产能否正常、安全的进行，直接或间接影响到产品的质量。这些重点设备本身是用来完成特定生产任务的应用系统，其自身没有任何的安全防护措施，可以通过网络对其进行任意的访问。一旦这些重点设备受到恶意攻击或者有人为误操作的影响，将会直接危及整个生产过程，影响生产安全，甚至发生事故。

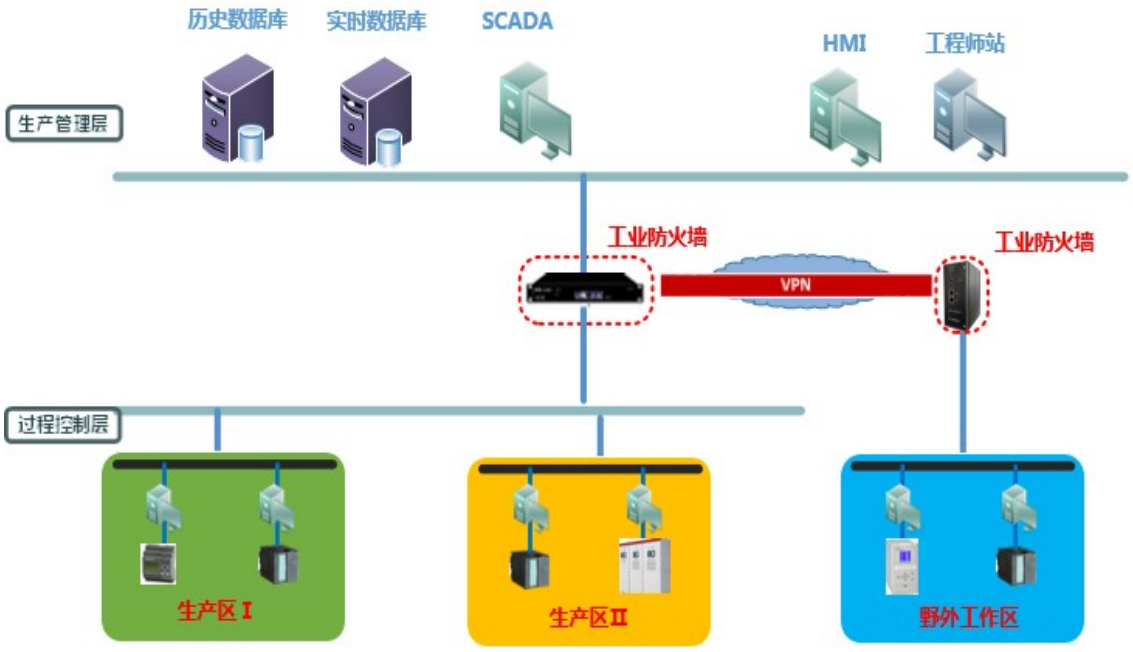
针对这些重点设备的特点可以在其前端部署 ISG 系列工业安全网关，限制可以访问它的 IP 地址、屏蔽非业务端口访问、过滤非法的操作指令、记录所有的访问和操作，对其进行全面的访问控制和安全防护。通过部署安全网关可以很好的实现对重点设备的事前安全防护、事中过滤检查和事后安全审计。



4.3 分散工业网络的安全互联

工业网络的设备可能分布于厂区各处，甚至野外、山区，由于网络基础设施的限制，经常需要通过租用公共的无线网络、卫星、GPRS/CDMA、4G 等公用网络传输线路实现与调度中心的连接和数据交换。公用网络没有足够的安全保护和加密措施，很容易出现网络窃听、数据劫持、第三人攻击等安全隐患，而且攻击者还可以利用公用网络作为攻击工业控制网络的入口，实现对于整个工业控制网络的渗透和控制。为了解决公用网络带来的安全隐患，用户通常都会租用或架设专用的通信线路，这样不但建设和运营成本高、而且需要专业的技术人员进行线路的保障和维护。

在这种应用环境下，可以在分散的作业区与公用网络接口的位置部署 ISG 系列工业安全网关。通过工业安全网关的部署可以对作业区内部的工业网络进行安全方面的保护，阻断来自公用网络的网络攻击，实现作业区网络的边界安全防护。


历史数据库
实时数据库
SCADA
HMI
工程师站
生产管理层
工业防火墙
VPN
工业防火墙
过程控制层
生产区Ⅰ
生产区Ⅱ
野外工作区