安企神

能源化工行业

网络准入控制解决方案

面向炼化 · 化工园区 · 油气田 · 储运 · 电力储能企业

让每一台终端合规入网，让每一次接入有据可查

目 录

01 项目背景 1

02 需求分析 2

03 方案设计 3

04 解决方案 5

第一部分 以身份与合规准入为主线 5

第二部分 以边界管控与运行保障为支撑 7

05 方案优势 9

06 方案价值 9

公司简介 11

01 项目背景

一套炼化装置从原油进厂到成品出库，中间是蒸馏、催化、加氢、储运一长串连续运转的环节。支撑这条流水线的不只是塔器和管线，还有一张分层运行的企业网络：办公网承载日常经营，管理网跑着 ERP 与 MES，生产控制网里是 DCS、SIS 和成百上千台仪表设备，视频监控网则挂满遍布厂区的摄像头。四张网彼此隔离，是行业多年的共识，也是安全生产的基本盘。

问题出在“隔离”这件事本身并不牢固。装置大修时，几支施工检修队伍集中进场，上百台外来笔记本一夜之间接入临时网络；设备厂商的调试工程师带着工具机直连工程师站；第三方运维远程接入组态机；巡检人员拿着自己的手机扫二维码报缺陷。这些动作每天都在发生，单看哪一件都合理，合起来却是同一个结果——网络里到底连着哪些设备、各自是谁带来的、什么状态，没有人说得清。

而生产网经不起试错。办公终端中了勒索软件，损失的是几台电脑；勒索软件顺着一条私接的网线进入生产控制网，代价就是装置非计划停车——大型炼化装置每停车一天，直接损失以百万计，还要叠加开停车物料损耗与安全风险。监管的要求也在收紧：《安全生产法》对危险化学品企业自动化控制系统提出了明确要求，等级保护 2.0、《关键信息基础设施安全保护条例》以及 2026 年 10 月起施行的公安部 176 号令，把生产网、管理网、内部专网全部纳入了监管视野，审批检查时“拿出接入记录”正在成为标准动作。

现实约束同样清楚：生产不能停，DCS 与 SIS 网络不能为了部署安全产品大改结构；大量仪表、摄像头；化工园区多厂区、多分公司并存，IT 与信息化往往只有几个人管着几千台终端。所以这个行业的安全建设，第一约束不是功能多少，而是“生产感觉不到”。

能源化工网络资产的三点特征

01 一台设备一个身份	02 生产网容错成本极高	03 接入主体高度混杂
一台操作员站、一个摄像头，背	外来施工、厂商调试、第三方运	设备一旦带病入网，蠕虫与勒索

01 一台设备一个身份	02 生产网容错成本极高	03 接入主体高度混杂
后对应的是装置的连续运转；任何一次误接入、误阻断都可能直接传导到生产现场。	维、访客与自有员工混在同一张网里，身份边界天然模糊。	软件沿生产网扩散的速度，远快于任何一次人工排查。

归根结底，能源化工企业要补的不是又一台防火墙，而是把住“进网的门”：谁要接入、是不是登记过的设备、状态合不合规、接进来能去哪个分区、事后能不能拿出记录。方案要做的，是把这些分散的动作收敛成一套准入体系、一张设备台账、一份可核查的记录。

02 需求分析

结合炼化、化工、油气田企业的网络分区与用网习惯，我们把共性问题归纳为四个方面。四个问题层层递进：设备看不见就认不了，认不了就查不严，查不严就管不住，管不住最后就说不清。

入网设备底数不清，台账靠人记

- 厂区里有多少台联网设备、各在哪个 VLAN、接哪台交换机哪个端口，多数企业拿不出实时台账；摄像头、NVR、打印机这类不产生流量的设备长期游离在管理之外。
- 装置大修、技改期间设备批量进出，人工登记赶不上变化，检修结束后的清网基本靠感觉。
- 新设备什么时候接入、接到哪个端口，事后无从追溯。

外来设备与访客缺乏统一入口

- 施工队、厂商调试、第三方运维各自带机入场，有的插网线就能用，有的问 Wi-Fi 密码，准入尺度全看接待人。
- 缺少一套入网申请与审批流程，谁批准的、批准用多久、用完有没有收回，都没有记录。

终端合规状态参差，带病设备直通内网

- 病毒库三年没更新、补丁长期未打、弱口令、违规装着破解软件的终端，照样能访问 MES 与文件服务器。
- 自带设备、老旧电脑、重装系统后的“裸机”，没有任何安全状态校验就直接入网。
- 一台带毒笔记本进入管理网，就可能成为横跳到生产网边界的跳板。

违规外联屡禁不止，事后举证能力弱

- 私接 4G 路由、随身 WiFi、笔记本开热点桥接内外网，是生产网被“打穿”最常见的一条路。
- 无线网卡、双网卡设备在隔离分区间随意摆渡，边界形同虚设。
- 上级检查或事故调查时，拿不出设备何时接入、何时离网、做过什么的完整记录。

03 方案设计

能源化工企业的网络准入，归纳起来是三个问题：哪些设备在网里，凭什么让它们进来，进来之后干了什么。因此方案不追求单点功能的堆叠，而是围绕一条主线展开——让每一台终端先被看见，再被认证，然后被体检，最终被安排到它该去的分区，并且全程留痕。

围绕这条主线，方案以“一个平台、五道闸门”组织能力：资产发现解决“看得见”，身份认证解决“认得了”，入网安检解决“够干净”，分区授权解决“去对地方”，审计留痕解决“说得清”。

一个平台 · 五道闸门

闸门	能力	解决的问题	实际效果
闸门 01	资产发现	看得见	主动扫描与被动侦听并行，全网设备秒级发现，台账自动生长

闸门	能力	解决的问题	实际效果
闸门 02	身份认证	认得了	人、机、账号三重校验
闸门 03	入网安检	够干净	补丁、端口、进程、弱口令逐项体检，不合格先隔离
闸门 04	分区授权	去对地方	按身份动态划分 VLAN 与权限，生产网最小化开放
闸门 05	审计留痕	说得清	接入、阻断、变更全程记录，检查与追溯当场拿得出

设计原则

- 旁路部署、不动网络结构——准入网关旁路接入，不换设备、不改变分区与业务流向，生产网通信路径零改动。
- 白名单为默认、生产网最小化开放——默认拒绝一切未登记设备；生产控制网只放行登记在册的工控终端与授权运维终端，外来设备一律走隔离区审批通道。

实施路径：三步走

第一步 资产盘点与建模	第二步 办公与管理网试点	第三步 生产网边界收口与制度固化
先扫描不动网：摸清全网设备底数，建立设备画像与白名单基线，完成策略规划。	在办公网与管理网启用认证与安检，跑通审批、隔离、修复三条链路，同步校准误判策略。	生产网边界逐分区启用 MAC 准入与端口级控制，将准入策略与检修、施工管理制度对接，形成可季度复核的闭环。

04 解决方案

方案能力分为两层：第一层是身份与合规准入主线，解决“谁能进网”；第二层是边界管控与运行保障底座，解决“进了之后怎么管、出了事怎么查”。两层共用一个管理平台，按需启用、逐步扩展。

第一部分 以身份与合规准入为主线

这一组能力回答“谁能进网”：从资产扫描、身份认证、入网安检、地址管理到访客审批，五个动作串成一条完整的进门链路，任何一个环节都不单独成立。

1.1 全网资产扫描与设备台账

准入的前提是看见。系统采用主动扫描与被动协议分析双技术并行，万台级设备快速完成发现，覆盖电脑、服务器、打印机、移动终端、摄像头、交换机、虚拟机，识别出操作系统、主机名、IP 地址、MAC 地址、开放端口、接入交换机，五十种以上常见网络服务自动识别。

- 台账自动生长：新设备接入即被发现并告警，设备从“靠人登记”变成“系统自己长出来”。
- 设备画像分类：按厂区、分区、品类自动归类，自有设备、外来设备一眼分清。
- 变更实时感知：私接小交换机、私改 IP、端口挪用等异常即时告警。



1.2 入网身份认证

身份是准入的第一道门。方案配合完成人、设备、账号的三重校验：员工终端用域账号加设备指纹认证；外来设备必须提交接入申请，核验身份后方可入网。

- IP-MAC 绑定：终端与地址、端口绑定，换设备自动断网，防止仿冒与顶替。
- 认证不改结构：无需更换网络设备、不影响业务系统与网络性能，认证失败只挡设备不动网络。

1.3 入网安检与自动修复

拿到账号、分到地址，不等于可以直接上网。入网前系统对终端逐项体检：杀毒软件安装与病毒库版本、系统补丁、开放服务与端口、运行进程、已装程序、账户口令强度、防火墙状态，摄像头与交换机等关键设备还支持自定义检查项。安检不合格的终端被引导进隔离区——网络只通修复服务器，修好后自动复检放行。

检查项	检什么	不合格怎么办

检查项	检什么	不合格怎么办
终端防护	杀软安装、病毒库版本、实时防护开启	引导安装更新，修复后复检
系统健康	补丁缺失、弱口令、异常账户	自动下发补丁，强制改密
行为环境	违规软件、异常进程、高危端口	进隔离区，整改后放行

1.4 IP 地址池与地址防篡改

图形化 IP 地址池把全网地址资源管起来：在线、离线、未使用、安全风险、安全阻断五类状态一目了然，地址与设备绑定保护，私改 IP 立即告警并可阻断。地址不再是散落的数字，而是与设备身份挂钩的管理坐标，冲突与顶替问题从源头消除。

1.5 访客与外来施工队伍准入

大修与技改是准入压力最大的时段。方案为外来设备建立专用通道：施工方提交设备清单与人员名单，多环节审批核验，严格与宽松模式按队伍风险等级选择；批准后发放带有效期的临时凭证，绑定设备、限定区域，到期自动失效并回收。访客终端只通互联网，摸不到生产网与管理网。

第二部分 以边界管控与运行保障为支撑

设备进了门，还可能从窗户翻出去——私接外联、乱开热点、跨区摆渡。这一组能力把边界管住，同时为准入体系提供终端加固与事后追溯的支撑。

2.1 违规外联与热点管控

对入网终端持续监测：私接 4G 路由、随身 WiFi、笔记本开热点桥接、无线网卡直连外部网络等行为实时检测、立即告警并可自动阻断；双网卡设备跨分区摆渡同样纳入管控。生产网被外部通道“抄后路”的问题，在这一层收口。

2.2 分区隔离与动态授权

与准入联动，终端认证通过后按身份动态划分 VLAN 与访问权限：办公终端到不了生产网，运维终端只能进授权维护的分区，外来设备锁定在隔离区。网络权限跟着身份走，而不是跟着网线走。

2.3 终端加固与运行保障

补丁统一管控与强制弱口令整改，持续压降终端自身的安全短板；软硬件变化报警让私拆、调拨、更换配件有据可查；远程协助让园区多厂区的日常运维不必再跑现场。

2.4 准入审计与台账报表

每一次接入、认证、阻断、隔离、放行都沉淀为记录，按设备、人员、时间、分区组合检索，从一条记录还原完整事件链。上级检查、事故调查、责任认定时，接入台账、审批单、阻断报表当场导出。



05 方案优势

能源化工企业评估准入方案时，最关心的无非三件事：会不会影响生产、要不要大改网络、检查时能不能拿出记录。

优势	说明
不动网络：旁路部署零改造	不更换网络设备、不改变分区结构、不影响业务系统与网络性能，生产网通信路径零改动。
混合准入：一种平台多种认证	802.1X、MAC、Portal、MAB、VLAN 等技术按分区混合启用，网络边界级、端口级、应用级阻断层层设防。
白名单默认：未登记进不来	默认拒绝一切未登记设备，外来设备走审批与隔离通道，从机制上杜绝“随手插网线”。
闭环可举证：接入全程留痕	资产、认证、安检、阻断、审批记录一体沉淀，对标等保 2.0 与关基条例要求，检查时当场出报表。
分级纳管：园区多厂区统一平台	总部与各厂区策略统一制定、分级下发，审批角色分离，贴合化工园区多主体运营的实际。

06 方案价值

价值	具体表现
底数“看得见”	全网设备一张实时台账，多少台、在哪、什么状态不再靠猜，大修期间设备进出全程可视。
入口“进不来”	未认证设备接上网线也没有业务权限，仿冒与顶替在认证环节即被拦截，网络大门从敞开变为刷卡进入。

价值	具体表现
终端“够干净”	带病终端先隔离修复再入网，勒索软件与蠕虫借道终端进入生产网的最常见路径被切断。
边界“管得住”	违规外联、私搭热点、跨区摆渡实时告警阻断，分区权限跟着身份走，生产网最小化开放。
举证“拿得出”	接入、审批、阻断记录完整可查，等保测评、上级检查、事故调查不必再临时翻台账。

这五条价值最终落在同一个目标上：让网络边界的管控从“出了事再查”变成“平时就管住”。对能源化工企业而言，这道管得住的门，本身就是安全生产防线的组成部分。

公司简介

石家庄安企神网络科技有限公司成立于 2015 年，是一家以研发信息安全类产品以及提供相关服务为主营业务的技术驱动型公司。

安企神软件是由该公司研发的终端安全管理系统，打造全生命周期一站式信息安全整体解决方案平台，集文档加密、电脑行为审计、终端安全管理、网络准入控制、敏感内容识别、IT 运维管理等 200+ 功能于一体，有效防护不当办公行为造成的数据泄露。

安企神软件深耕终端安全与数据防泄密领域十余年，拥有 300 余家合作伙伴，服务万余家政企客户，累计覆盖终端超 1000 万台，广泛应用于政府、金融、运营商、制造、能源、教育、医疗等行业的大型知名单位和机构，涵盖衣食住行各行各业。

ANQISHEN
400-666-2563
www.wgj7.com
河北·石家庄
安企神软件®