安企神制造行业

文档防泄密解决方案

面向机械装备 · 汽车零部件 · 电子制造 · 精细化工 · 模具加工企业

让每一张图纸、每一份工艺文件，都留在它该在的地方

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 以文档防泄密为主线.....5

第二部分 以终端与通道管控为底座.....9

05 方案优势.....10

06 方案价值.....10

公司简介.....12

01 项目背景

一台高端装备从接单到交付，中间要经历方案设计、详细设计、工艺编制、工装模具、试制验证、批量生产一长串环节。设计部门产出成百上千张图纸和三维模型，工艺部门把它们变成工序卡片、作业指导书和数控程序，采购与生产环节又生成 BOM 清单、外协订单与检验报告。这些文件分布在几百台办公电脑、几十台产线工控机和若干台文件服务器上，构成了一家制造企业最真实的家底。

制造业文档的价值，往往在流失之后才被准确估价。一套成熟的冲压模具图纸，背后是数轮试模换来的参数积累；一份经过验证的工艺配方，直接决定产品的良率与成本；一条完整的产品 BOM 加上供应商价格体系，足以让竞争对手省掉两年的摸索。设备折旧了可以更新，但一套设计工艺文档被完整拷走，带走的是几代产品迭代省下的弯路。

外部的要求也在收紧。《数据安全法》对重要数据的全流程管理提出了明确义务；下游主机厂对供应商的体系审核中，文档管控与信息安全是固定条款；越来越多客户在招标阶段就要求投标方出示访问控制与操作留痕能力。泄密的路径同样在演化：设计员用微信把图纸发给外协厂，采购把报价单存进个人网盘，工艺员离职前把整套工艺文件拷进移动硬盘——这些动作单件看都像日常工作，连起来就是一条完整的泄密链。

但制造业安全建设有自己独特的约束：生产不能停，产线终端不能动辄重启，车间网络环境复杂，一线员工素质参差。所以制造业的文档防泄密，第一约束不是功能多少，而是不能干扰正常生产与办公。

制造企业文档资产的三个特点

01 图纸即核心资产	02 一份文件全链流转	03 终端与人员复杂
一套图纸、一份工艺文件背后是	一张图纸要从设计流到工艺、采	办公电脑、产线工控机、出差笔

01 图纸即核心资产	02 一份文件全链流转	03 终端与人员复杂
数轮试制与工艺积累，单个文件的价值远超其载体。	购、外协、生产、质检，经过的部门和人越多，失控点越多。	记本并存；设计、工艺、一线员工、外协人员混杂，管控颗粒度必须精细。

02 需求分析

结合制造行业研发、工艺、生产、供应链各环节的协作方式，我们把制造企业文档防泄密的共性问题归纳为五个方面。它们不是五个孤立的缺口，而是同一条链上的五个环节：文档散在终端，从多条出口流出，事后说不清楚。

设计与工艺文档散落在终端，谁看、谁拷、谁发没有统一口径

- 二维图纸、三维模型、工艺文件、数控程序以明文存在个人工作目录，同一张图纸在多个终端有多个版本。
- 文件服务器与本地磁盘之间频繁互拷，一套模具图纸在全厂多处留有副本，哪份是受控版本没人说得清。
- 部门间协作靠共享目录、即时通讯和移动硬盘，文件一旦离开部门边界就完全失控。

图纸外发链条长，客户、供应商、外协各有各的通道

- 向客户提供图纸方案、向供应商发出询价资料、向外协厂发放加工图纸，是企业运转的日常，管控目标不是"发不出去"，而是"发出去的那份可控"。
- 外协加工涉及大量跨企业数据交换，图纸到了外协厂手里，能否另存、能否转发、用完能否收回，多数企业没有答案。
- 报价单、BOM、供应商信息在采购与销售手里流转，属于最容易被忽视的高敏感文档。

办公终端与产线终端混杂，环境差异大，一刀切必然误伤

- 设计端是高性能图形工作站，依赖 CAD、PLM 等大型软件；产线是工控机与嵌入式终端，承担着 MES 读卡与设备通讯；管理端是普通办公电脑，三类环境要共存于同一套策略之下。
- 加密若介入读写路径过深，CAD 打开大装配出现卡顿，一线就会想办法绕开管控。

打印、拷贝、拍照等物理出口多，缺少技术约束

- 图纸打印出来带出车间、U 盘插上就拷走、手机对着屏幕拍一张，是三种最常见也最难凭制度约束的出口。
- 保密协议写得再细，出了事拿不出终端侧记录，举证和追责都落不了地。

审计与举证能力薄弱，客户验厂与内部追责都吃力

- 日志分散在各终端与服务器，被问到"这套模具图纸最近半年被谁拷过"，只能人工排查。
- 客户验厂要的管控记录靠临时手工整理，无法常态化输出。

03 方案设计

制造行业的文档安全问题，本质是三句话：文档不受控、出口不受限、行为不留痕。因此方案不追求功能堆叠，而是围绕一条主线展开——让文档在企业内部自由流转、离开授信边界无法使用、每一次流转有迹可循。

围绕这条主线，方案以"一个平台、四道防线"组织能力：文档加密解决"带走也没用"，通道管控解决"带不走"，终端治理解决"从哪台机器带"，审计溯源解决"带走了能查到"。

一个平台 · 四道防线

防线	能力	解决的问题	实际效果

防线	能力	解决的问题	实际效果
防线 01	文档加密	可用不可带走	图纸工艺文件在内部正常打开编辑，离开授信环境即为乱码
防线 02	通道管控	带不走	打印、U 盘、即时通讯、邮件、截屏拍照，逐条出口设策略
防线 03	终端治理	摸得清	资产、软件、外设、准入，一台终端一张底账
防线 04	审计溯源	查得到	记录、检索、报表与取证，把"说不清"变成"拿得出"

三条设计原则

- **按部门分域、按密级授权**——设计、工艺、采购、财务各成安全域，跨域访问以授权代替解密，普通账号打不开高密级工艺文件。
- **一个客户端、一套管理端，不改变现有作业习惯**——办公电脑与产线终端统一纳管，加密在驱动层完成，CAD 与办公软件的使用方式不改。
- **生产优先，能灰度**——策略先在非关键部门试点，产线终端单独分组、单独策略，安全建设不以影响交付为代价。

实施路径：三步走

第一步 部门试点	第二步 全厂推广	第三步 制度固化
选设计或工艺部门先行部署，跑通加密、外发、审计三条主链路，同步完成性能基线测试。	覆盖研发、生产、采购、财务全部办公终端与产线工控机，策略由总部集中下发、按岗位差异化配置。	把策略与保密制度、外协协议、客户验厂要求逐条对应，形成可定期复核的管理闭环。

04 解决方案

方案能力分为两层：第一层是文档防泄密主线，解决"图纸和工艺文件怎么管"；第二层是终端与通道管控底座，解决"文档靠什么机器承载、从哪条通道进出"。两层能力共用一个客户端与一个管理平台，按需启用、逐步扩展。

第一部分 以文档防泄密为主线

这一组能力回答"核心文档怎么管"：从加密、设计工具适配、外发管控、打印与屏幕防护、敏感识别到行为审计，六个动作串成一条从文档产生到归档的链路。

1.1 文档透明加密

图纸的价值在内容，不在它存在哪个目录。第一个动作是让文档本身带锁：加密在驱动层完成，保存即密文，在授信环境内正常打开、编辑、出图，一旦离开授信环境，打开就是乱码。

加密模式	适用岗位与场景	实际效果
透明加密	设计、工艺等核心研发岗	新建保存即密文，内部正常使用，外发为乱码
智能加密	生产、质检等读取多、外发少的岗位	按进程与文件类型判定，命中敏感规则才加密
只读	提供给客户的图纸方案、供应商报价资料	可看不可改、不可另存，防止二次扩散
落地加密	客户来图、外协回传、供应商交付件	落到本机即转密文，转发到别处无法打开

实施要点：按岗位分配模式，核心研发岗透明加密，产线与办公岗智能加密；采用国密算法与分级密钥，按部门与密级分级管理，满足合规审查对存储机密性的要求；例外清单可维护，CAD 安装目录、PDM 缓存目录经审批加入例外，避免误伤工具链。

1.2 设计工具适配

安全方案如果让 CAD 打不开大装配、让 PLM 检入检出差错，一定撑不过一个项目周期。第二个动作是把管控做进设计工具的读写路径。

- 主流 CAD 与设计软件：AutoCAD、SolidWorks、UG NX、CATIA、CAXA 等常见设计与工艺软件经过适配，加密后打开、编辑、出图体验不变。
- PLM/PDM 协同：检入检出、版本流转过程中文件保持密文落盘，授权终端与授权进程正常访问，不改变原有权限模型。
- 性能保障：大型装配文件与海量小文件分别优化，上线前后对同一套图纸的打开耗时建立基线。

1.3 外发管控与供应链协同

制造业的分工决定了图纸必须流动：发给客户确认、发给供应商询价、发给外协厂加工。管控的目标不是"流不出去"，而是"出去的那一份可控"。外发四步：申请、审批、受控、留痕。

环节	动作	落地方式
申请	说明用途、接收方、文件清单与有效期	客户端发起，自动带出文件指纹与大小
审批	部门负责人 / 研发负责人分级审批	超出预设范围自动升级，驳回须填原因
受控	生成受控外发文件，原文件不解密	限定打开次数与有效期、绑定设备、禁止打印、页面叠加水印
留痕	记录谁、何时、发给谁、打开了多久	与审计模块打通，可回溯到具体项目

三类典型场景：客户图纸交付以只读受控文件发出，到期自动失效，客户侧无法另存转发；外协加工图纸走专用受控通道，加工周期结束文件即锁定；供应商报价与 BOM 资料按最小必要原则拆分发放，避免整套数据一次性外流。邮件与即时通讯外发实行白名单放行、其余审批；出差与驻场支持可申请离网授权，到期自动失效。

1.4 打印、外设与屏幕防护

文档落到纸面、落到介质、落到另一台机器上，就再没有技术约束。能做的只有三件事：事前管住谁有权输出，事中让输出带上痕迹，事后留得下输出过什么。

通道	主要风险	管控方式
打印	图纸、工艺卡打印外流	审批、打印水印、内容留存，共用打印机按部门绑定
U 盘与移动硬盘	整目录拷贝带走	禁用、只读、只写、白名单四种授权；专用加密 U 盘仅限授信终端打开
即时通讯与网盘	微信发图、网盘备份	禁止指定程序外发文件，敏感文档外发即阻断并告警
截屏与拍照	屏幕内容被手机拍走	截屏管控、屏幕点阵水印，检测到拍照自动锁屏

屏幕是办公终端上最后一道、也最容易被忽略的出口。屏幕水印叠加姓名、工号与时间，拍照即留痕；点阵水印在图纸被翻拍后仍可溯源到人。当员工知道屏幕上始终带着自己的名字，随手拍这个动作本身就会变得犹豫。

1.5 敏感文件识别与防勒索备份

分类分级是文档治理的起点，落到终端上要先回答三个具体问题：哪些文件里有核心图纸与工艺，它们躺在哪台机器上，现在是不是明文。

- 敏感文件扫描：按自定义敏感词与文件特征扫描全终端，命中即告警，形成敏感文档台账。

- 敏感信息报警：图纸外发、批量拷贝触发实时告警，缩短响应时间。
- 文档防勒索与自动备份：文件删除、修改自动备份，遭遇勒索病毒时可快速恢复，安全与容灾一并解决。

识别是起点，策略才是终点：扫描清单要变成规则——哪些目录必须加密、哪些岗位只能只读、哪些文件外发必须审批，同时避免过度管控，公开资料保持原样。

1.6 行为审计与离职风险预警

一家几百人的制造企业，一天产生的行为记录数以万计。审计的价值不在于"都记下来"，而在于要的时候找得到：文件操作、打印、外设、邮件、即时通讯、网页、程序统一采集，断网续传；按人、时间、部门、文件类型组合检索，从一条记录还原整条事件链；审计报表与取证材料随时输出，客户验厂当场拿得出记录。

三类值得关注的信号：离职前行为——离职流程发起前批量下载、集中压缩、频繁访问非本人部门目录；异常外发——非工作时段大量外发、向个人邮箱或网盘发送、审批被驳回后改用其他通道；越权访问——跨部门访问核心工艺目录、频繁使用截屏工具。



第二部分 以终端与通道管控为底座

文档之所以能被带走，前提是有终端可以承载、有通道可以出海。终端与网络本身管不清，文档防线就成了空中楼阁。

- **资产台账与变更报警**：全网扫描生成软硬件台账，硬盘、内存、外设更换即时报警，报废调拨有据可查。
- **软件管控与正版合规**：设计软件与办公软件统一分发，禁止私装来源不明程序，破解版工具远程清理，降低版权与供应链风险。
- **违规外联与网络准入**：私接互联网、私搭热点立即告警并可阻断；准入网关校验用户身份与设备身份，合规才入网。
- **补丁与弱口令治理**：补丁统一管控、弱口令强制整改，堵住终端最基础的加固短板。
- **远程协助与运维分发**：故障远程处理、文件与通知批量分发，多厂区运维不必等上门。



05 方案优势

制造企业选型时最常问的三个问题：会不会拖慢设计与生产、要不要改现有环境、出了事能不能拿出证据。对应的答案，构成了这套方案的基本盘。

优势	说明
一体化：一个客户端，一个平台	加密、审计、通道管控、准入、跨网交换在同一客户端内实现，不必为每类需求装一套系统
不影响作业：不动设计工具链	加密在驱动层完成，CAD、PLM、办公软件调用方式不变，性能有基线
闭环：事前、事中、事后	事前以加密预防，事中以通道阻断，事后以审计取证，三段能力串成一条链
分域：部门制隔离	以部门为单元划安全域，跨域越权访问在客户端侧即被拦住，贴合制造企业组织方式
可举证：对标体系与验厂要求	访问控制、安全审计、数据保密性措施可映射等保2.0 条款，支持国密算法，验厂时能出报表
可扩展：多厂区统一纳管	总部与各厂区在同一平台分级授权，策略统一制定、分级下发，运维与审计角色分离

06 方案价值

价值	具体表现
核心图纸"可用不可带走"	图纸与工艺文件在内部自由流转，离开授信环境即为乱码，"拷一份带走"从技术上失效

价值	具体表现
出口"可管可查"	打印、外设、外发、屏幕四类出口都有策略与记录，堵住最常见的几条泄密路径
外发"出去的可控"	客户、供应商、外协三条外发链路全部受控留痕，交出去的文件到期收回、翻拍可溯源
举证"拿得出"	日志、报表与事件链当场调取，客户验厂、内部追责不必再动员全公司翻台账
生产"不降速"	性能有基线、策略可灰度、异常可回退，安全不以影响交付为代价

这五条价值指向同一件事：把过去依赖保密协议、依赖人盯人、依赖离职面谈的管理方式，换成可持续运行的技术机制。制度写在纸上，机制跑在终端上，两者合起来才叫"管得住"。

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®