安企神 IC 设计行业

数据防泄漏解决方案

面向芯片设计 · 晶圆制造 · 封装测试 · IP 与 EDA 企业

让核心数据在内网安全流转，让每一次流转可追溯

目录

01　项目背景 1

02　需求分析 2

03　方案设计 4

04　解决方案 5

　　第一部分　以数据防泄漏为导向 5

　　第二部分　以终端与通道管控为支撑 11

05　方案优势 12

06　方案价值 12

公司简介 14

01 项目背景

一颗 SoC 从立项到量产，要走完架构定义、RTL 编写、功能验证、逻辑综合、布局布线、物理验证、流片、封装测试一长串环节。几百名工程师在几百台终端上工作两三年，产出是几千万行代码、上百 GB 版图数据，和一套只有自己团队看得懂的验证环境。这些东西不占厂房、不压库存，全部躺在一个几十 TB 的存储里，却构成了一家 IC 企业几乎全部的资产——设计公司如此，IDM 与封测厂亦然。

芯片公司的账本上，最贵的不是服务器和工位，而是这些文件背后的研发投入与试错成本。一颗中高端芯片的研发费用以亿元计，一次流片就是数千万元，设计数据库里沉淀的则是几代产品的架构经验与工艺适配参数。设备可以再买，一套被完整带走的设计数据库却没有任何办法重建。

竞争与合规的压力同时压过来。出口管制、实体清单、EDA 与 IP 的供应限制，把“技术自主”从口号变成了每周都要面对的问题；团队流动率居高不下，同一批工程师在几家公司之间流转，人走了经验跟着走很正常，设计文件也跟着走就完全是另一回事。车规客户看 AEC-Q100 与 ISO 26262 体系，也看设计数据如何隔离；客户审厂会直接要求出示访问控制记录与操作日志；《反不正当竞争法》对商业秘密的保护、《数据安全法》对重要数据的管理要求、ISO/IEC 27001 与等级保护对访问控制和安全审计的规定，最终都要落到“能不能拿出记录”这一件事上。

泄密的路径也在变。十年前是 U 盘和邮件附件，现在更多是这几种：把工程目录打包上传个人云盘；把代码推到自己的 GitHub 私有仓库；用远程桌面连回研发网“加班”；在外协与高校联合实验室的边界上两边各有各的口径；离职前两周批量下载、压缩、改名、分卷外发。这些动作单看都不刺眼，连起来就是一条完整的输出链路。

现实投入却常常不对称。芯片公司愿意为 EDA license 和算力付高价，愿意为 IP 付授权费，安全预算却排在后面。原因不难理解：安全软件一旦拖慢编译、卡住仿真、拦住正常的工具调用，研发第一时间就会要求卸载。所以这个行业的安全建设，第一约束不是功能多少，而是“研发感觉不到”。

IC 设计数据资产的三点特征

01　单点价值极高	02　泄露即不可逆	03　协同边界模糊
一份网表、一套版图，背后是数亿元研发投入与几代产品的工艺积累，单个文件的价值远超普通商业文档。	IP 一旦流出无法召回，也无法靠重新设计补救；对手拿到的不只是代码，还有你走过的弯路。	IC 企业要与 IP 供应商、外协团队、代工厂、封测厂、客户样片团队交换数据，上下游分工越细，数据边界越不封闭。

说到底，IC 行业的数据安全不是“再装一套软件”，而是让核心数据从创建到归档的每一次流转都处在可控范围内：谁能打开、能不能拷、能不能发、发给谁、发出去之后还能不能追。方案要做的，是把零散的管控动作收敛成一套规则、一个平台、一份可核查的记录。

02　需求分析

结合 IC 行业设计、制造、封测各环节的终端环境与协作方式，我们把共性问题归纳为五个方面。它们不是五个独立的缺口，而是同一条链路上的五个环节：数据散在终端，从多条出口流出，事后又说不清楚。

设计数据散落在研发终端，谁看、谁拷、谁发没有统一口径

- RTL、网表、脚本、验证用例、波形以明文存放在个人工作目录，同一模块在不同终端存在多个“最新版”。
- 共享存储与本地磁盘之间频繁拷贝，一份 GDS 或多套 PDK 在多个位置留下副本，哪份是受控版本没人说得清。
- 跨团队协作靠 U 盘、即时通讯、邮件和临时共享链接，文件一旦离开研发网就完全失控。

研发环境特殊，安全措施稍有不慎就会拖慢工具链

- Windows 与 Linux 双栈并存，设计端依赖高性能工作站与大内存服务器，制造与封测端还有 MES 配套终端与产线工控机，客户端必须同时覆盖多类环境。
- 编译、综合、仿真、DRC/LVS 都是长任务、高 IO，加密若介入读写路径过深，make 一次多花几十分钟，团队就会想办法绕开。

- EDA 安装目录、临时目录、license 服务、容器与虚拟机镜像读写特征各异，一刀切的策略必然误伤。

交付与协同出口多，流片、IP 授权、外协各有各的通道

- 设计端流片要向代工厂传 GDS/OASIS、DRC/LVS 报告与 test pattern，制造与封测端要向客户和协作方传工艺数据、良率报告与测试程序，数据量以几十 GB 计，常通过专线、FTP 或移动硬盘完成。
- IP 授权与评估需要向潜在客户提供部分设计资料，既不能给全套，也不能只给一张框图。
- 外协团队、高校联合实验室、异地研发中心接入研发网，账号与设备缺乏统一校验；客户样片与 datasheet 又在销售与 FAE 手里流转。

人员流动带来的带离风险，缺少可预警的信号

- 离职前集中下载、批量压缩、分卷改名、上传个人网盘，事后只能看到结果，看不到过程。
- 把工程代码推到个人代码托管平台、把仿真脚本发到技术论坛求助，是常见小动作，对 IP 却是实质性泄露。
- 保密协议与竞业条款写得再细，举证时缺少终端侧记录，很难形成完整证据链。

审计与举证能力薄弱，客户审厂与内部追责都吃力

- 日志分散在文件服务器、版本库、网关、堡垒机各处，缺少按项目维度的统一检索入口。
- 被问到“这个项目的版图数据过去半年被谁拷走过”，只能人工排查，答复周期以天计；客户 audit 要的报表靠临时手工汇总，无法常态化。
- 另外，多站点也是现实：总部、异地研发中心、海外分部、并购团队并存，终端从高性能工作站到仿真服务器、机台配套 PC 跨度很大，而 IT 与信息安全往往只有几个人。

03 方案设计

IC 行业的数据安全问题，本质是三句话：资产不受控、通道不受限、行为不留痕。因此方案不追求功能项的堆叠，而是围绕一条主线展开——让核心数据始终处于可控状态，让每一次流转都可追溯，让管控动作落在既有的研发与生产流程之内。

围绕这条主线，方案以“一个平台、四道防线”组织能力：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 01	数据加密	可用不可带走	设计文件在研发网内正常打开、编译、流转，离开授信环境即为乱码
防线 02	通道管控	带不走	外设、打印、外发、截屏与拍照，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

- 按项目分域、按 IP 密级授权——以项目而非部门作为隔离单元，一个项目组一套安全域，人力随项目增减；项目内再按密级细分，低密级账号打不开高密级文件，跨项目协作以授权代替解密。

- 一个客户端、一套管理端，不动研发工具链——终端侧只装一个客户端，Windows 与 Linux 同源；管理侧只有一个后台，策略按项目组、站点、岗位批量下发。加密在驱动层完成，编译脚本与 EDA 调用方式一律不改。
- 性能与稳定优先，能灰度、能回退——大文件与小文件、顺序与随机读写分别压测；上线按项目组灰度，异常可单机回退。安全的底线是不影响流片节点。

实施路径：三步走

第一步　单项目试点	第二步　研发域推广	第三步　流程与制度固化
选一个核心研发项目组先行部署，跑通加密、外发、审计三条主链路，同步完成性能基线测试。	覆盖设计、工艺、测试与封测协同团队，异地站点与产线终端统一纳管，策略由总部集中下发。	把策略与 IPD 流程、保密制度、客户 audit 应答逐条对应，形成可季度复核的闭环。

04　解决方案

方案能力分为两层：第一层是数据防泄漏主线，解决“设计文件怎么管”；第二层是终端与通道管控底座，解决“数据靠什么机器承载、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　以数据防泄漏为导向

这一组能力回答“设计文件怎么管”：从加密、工具链适配、外发管控、外设输出、敏感识别、屏幕防护到行为审计，七个动作串成一条从产生到归档的链路，任何一个环节都不单独成立。

1.1　设计数据透明加密

设计文件的价值在内容，不在它放在哪个目录。所以第一个动作是让文件本身带锁：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、编译、仿真，一旦离开授信环境，打开就是乱码。

加密模式与适用场景

加密模式	适用岗位与场景	实际效果
透明加密	设计、版图、工艺等核心研发与工程岗	新建与保存即密文，内网正常使用，外发为乱码
智能加密	验证、测试、品质等读取多、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	提供给客户评估的资料、供应商协作件	可看不可改、不可另存，防止二次扩散
落地加密	客户来图、IP 供应商交付件、代工厂回传数据	落到本机即转为密文，转发到别处无法打开
不加密	公共资料、开源代码目录、演示样机、离职人员	保持原有习惯，由外发与审计手段兜底，加密不可看

实施要点

- 按项目分配模式：核心项目组启用透明加密；读取为主、外发少的岗位用智能加密；对外评估件设为只读；客户与供应商来件用落地加密。
- 国密算法与分级密钥：采用 SM3/SM4，按项目与密级分级管理密钥，既满足密评对存储机密性的要求，也为客户 audit 提供可说明的技术口径。
- 例外清单可维护：EDA 安装目录、license 临时文件、编译中间产物目录经审批后可加入例外，避免误伤工具链。

> 文件在终端始终是密文，出口决定结果——研发网内的授信终端与授权工具里正常使用；经 U 盘、邮件、截图、个人网盘等非授信出口离开，得到的只是乱码，或被阻断并留下记录。

1.2 研发工具链适配

安全方案如果让编译变慢、让仿真排队、让 EDA 报错，一定活不过一个流片周期。所以第二个动作不是加管控，而是把管控做进工具链的读写路径里。

- Linux 工作站与服务器：客户端支持主流发行版与国产操作系统，命令行、脚本、调度系统调用方式不变，不依赖图形界面。
- 共享存储与 NFS：共享目录内文件以密文落盘，授权终端与授权进程正常访问；跨站点挂载同样按策略生效，不改变原有权限模型。
- 容器与虚拟环境：镜像与挂载卷按目录策略处理，编译容器内的读写不受影响，避免“一进容器就报错”的常见问题。

让长任务不受影响

- 大文件优先：GDS、OASIS、波形库等超大文件的顺序读写做专项优化，流片前数据打包时间不因加密显著延长。
- 小文件不吃亏：一套验证环境动辄数万文件，客户端对海量小文件做批量化处理，避免逐文件握手带来的延迟累积。
- 性能可观测：上线前后对比同一套工程的编译与仿真耗时形成基线，出现劣化可定位到具体策略并单机回退。

1.3 供应链协同与外发管控

芯片产业链的分工决定了数据必须流动：设计交给代工厂流片、交给封测厂测试、交给客户评估、交给外协团队开发，工艺与量测数据在制造与封测环节之间往复。管控的目标不是“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	项目负责人 / IP 负责人 / 法务分级审批	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

环节	动作	落地方式
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

- 流片与量产交付：向代工厂、掩膜版厂、封测厂提交的数据包走专用通道与白名单，传输前后校验完整性，交付清单与审批单一一对应，避免“多给了一个 layer”这类事故。
- IP 授权与评估：给潜在客户的资料以只读受控文件交付，限定查看次数与到期时间，客户侧无法另存与转发。
- 外协与联合实验室：为外协团队建立独立安全域，只开放其负责模块的目录权限，账号与设备双重校验，项目结束即回收。

邮件与离线

邮件白名单放行已备案的代工厂、封测厂与客户邮箱，其余外发仍需审批；出差与客户现场支持可申请离网授权，到期自动失效。

1.4 外设与输出通道

设计数据落到纸面、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
U 盘与移动硬盘	整目录打包带走	禁用、只读、只写、白名单四种授权；加密 U 盘仅限授信终端打开
光盘刻录	交付与备份两用，事后无记录	授权使用、刻录留档、内容留存
打印与复印	版图截图、测试报告外流	审批、水印、内容留存，共用设备按岗位绑定
烧录与调试接口	FPGA 比特流、样片固件被读出	编程器与调试工具白名单，操作

通道	主要风险	管控方式
		留痕
测试机台与工装	产线侧数据外带	机台配套终端单独分组，接口与目录严格限定

水印可追溯，纸面与屏幕叠加姓名、工号、项目代号与时间，文件流出后能锁定到人；内容可复核，不仅记录“打印了几页”，还留存输出文档；分级豁免，公共资料与已公开 datasheet 不必层层审批。

1.5 敏感内容识别与分类分级

分类分级是数据治理的起点，落到终端上要先回答三个具体问题：哪些文件里有核心 IP，它们躺在哪台机器上，现在是不是明文。

环节	做什么	输出
01 数据源	扫描研发终端、共享存储、文件服务器	待检文件清单与分布
02 识别	关键词、正则、文件指纹	命中规则的文件与置信度
03 标记	打上项目、IP 类型、密级标签	敏感文件台账
04 处置	补加密、告警、阻断外发、纳入分级	处置结果与责任人

常见敏感特征（规则库可按项目自定义）

项目代号与芯片型号命名、工艺节点标识、工艺配方与良率数据特征、IP 核名称与版本号、GDS/LEF/OASIS/LIB/DB 文件指纹、RTL 顶层模块名、DFT 与 ATPG 向量、封装与 pinout 定义、尚未公开的 datasheet。

不少公司做过一轮敏感文件扫描，得到一份长长的清单，然后就没有然后了。清单本身不产生价值，价值在于把清单变成规则：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。识别是起点，分级与策略才是终点。同时也要避免过度管控——只对命中规则的目录加密，开源代码与公共库保持原样。

1.6 屏幕与成像防护

加密挡住了文件，却挡不住一部手机。屏幕是研发终端上最后一道、也最容易被忽略的出口——尤其在版图评审、架构讨论和客户 demo 的场合。

出口	典型动作	应对
肉眼与相机	评审会上拍版图、拍架构图	拍照锁屏，屏幕水印（姓名、工号、项目代号、时间），拍照即留痕
截屏与录屏	一键保存、一键转发，扩散无痕	截屏管控，仅在受控文档区域遮蔽，普通页面不受影响
复制与拖拽	一段 RTL、一个参数表，三秒搬走	剪贴板与拖拽管控，禁止带入外部程序或网页

版图工程师在评审会上用手机拍下屏幕上的 floorplan，发到几百人的技术交流群里求助——这不是恶意窃密，却同样是核心 IP 外流，既难用法条约束，也很难靠人盯人发现，只能在动作发生的瞬间留下可追溯的痕迹。当员工知道屏幕上始终带着自己的名字与项目代号，随手拍这个动作本身就会变得犹豫。

1.7 行为审计与离职风险预警

一家几百人的 IC 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。

环节	内容
统一采集	文件操作、外设、打印、邮件、即时通讯、网页、程序、剪贴板、远程操作；客户端缓存，断网续传
聚合检索	按人、时间、项目、关键词、文件类型组合检索，

环节	内容
	从一条记录还原整条事件链
输出取证	审计报表、事件链条、检查佐证、责任认定材料

三类值得关注的信号

- 离职前行为：离职流程发起前三十天内批量下载、集中压缩、改名分卷、频繁访问非本人模块目录。
- 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：跨项目访问核心 IP 目录、尝试打开超出密级的文件、频繁使用截图与录屏工具。

一次客户 audit 或一次内部追责，如果只能回答“我们查一下”，结果往往已经是被动。能当场调出记录、说清路径、指明责任人的团队，处理成本完全不是一个量级。

第二部分　以终端与通道管控为支撑

数据之所以能被带走，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——资产不明、软件随意、外设失控、谁能入网没门槛——数据防线就成了空中楼阁。所以这一组能力是防泄漏的底座：先把承载设计数据的终端摸清楚，再把每一条进出通道收口。

能力	解决什么
2.1　资产台账与变更报警	全网扫描生成软硬件台账；内存、硬盘、网卡、外设更换即时报警，报废、调拨、私拆都有据可查。
2.2　软件标准化与 license 合规	EDA 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。
2.3　外设与移动介质	U 盘、光驱、蓝牙、USB 外设分类管控；加密 U 盘仅限授信终端打开，物理出口逐一收口。
2.4　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、设备身份与安全状态，合规才入网。

2.5　备份、补丁与远程运维	文件删除与修改自动备份，配合文档防勒索；补丁统一管控、弱口令强制整改；远程协助让异地站点不必等上门。

05　方案优势

IC 企业选型时最常问的三个问题：会不会拖慢研发与生产、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、维护一套账号体系。
不影响办公：不动研发工具链	加密在驱动层完成，编译、仿真、EDA 调用与共享存储访问方式不变；Windows 与 Linux 同源客户端，性能有基线、可回退。
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，而不是各自独立的工具箱。
分域：项目制隔离	以项目为单元划安全域，人力随项目增减，跨项目越权访问在客户端侧即被拦住，贴合芯片研发的组织方式。
可举证：对标体系与审厂要求	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，客户 audit 时能出报表。
可扩展：多站点统一纳管	总部、异地研发中心、海外分部在同一平台分级授权，策略统一制定、分级下发，运维、安全、审计角色分离。

06　方案价值

价值	具体表现

价值	具体表现
核心 IP“可用不可带走”	设计文件在公司内部自由流转，离开授信环境即为乱码。加密不改变研发习惯，却让“拷一份带走”这条路从技术上失效。
出口“可管可查”	外设、打印、外发、屏幕、烧录五类出口都有策略与记录，堵住的不是某一个漏洞，而是最常见的几条泄密路径。
举证“拿得出”	日志、报表与事件链可以当场调取，客户 audit、投资方尽调、内部追责都不必再动员全公司翻台账。
研发“不降速”	性能有基线、策略可灰度、异常可回退，安全不以拖慢流片节点为代价，制度才留得下来。
运维“从跑腿到平台”	资产、软件、补丁、故障在同一平台处理，异地站点不必等上门，几个人的 IT 团队也能管住几百台终端。

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