安企神

半导体行业

数据防泄密解决方案

面向芯片设计 · 晶圆制造 · 封装测试 · EDA 与 IP 企业

让每一份工艺与设计数据带锁流转，让每一次流转有据可查

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 6

1.1 核心数据透明加密 6

1.2 半导体工具链与系统适配 7

1.3 供应链协同与受控外发 7

1.4 数据出口管控与水印追溯 8

1.5 敏感内容识别与分类分级 9

1.6 行为审计与追溯取证 10

05 方案优势 11

06 方案价值 12

公司简介 13

01 项目背景

半导体是典型的「重投入、轻资产形态」行业：一家 Fabless 公司的全部家当，可能就是几套工艺库、几十万行 RTL、上百 GB 的版图与仿真数据；一家晶圆厂的命脉，则浓缩在一份份工艺配方、光罩数据与良率参数里。这些数据不体现在资产负债表上，却直接决定了企业十年的技术积累能否延续。一颗先进制程芯片从立项到量产动辄数亿元投入，一次流片成本以千万计，而晶圆厂一条产线的工艺调优往往要耗费数年——支撑这一切的核心数据一旦完整外流，损失没有任何补救手段。

与高价值形成反差的，是数据在产业链上的高频流转。芯片设计公司要把版图数据交给代工厂流片、把测试程序交给封测厂、把评估资料交给潜在客户；晶圆厂要向设备与材料供应商开放部分参数，向客户回传量测与良率数据；封测厂要在多个客户之间切换产线程序。分工越精细，数据出手的次数就越多，每一次出手都是一次暴露面。此外，IDM 与代工厂普遍存在多基地运营，设计中心、晶圆厂、封测厂分布在不同城市甚至不同国家，数据在站点之间日夜穿梭。

监管与客户的压力同样具体。《数据安全法》与《反不正当竞争法》对重要数据和商业秘密提出了明确的管理与举证要求，等级保护 2.0 把访问控制与安全审计列为基本项；车规客户在审厂时不仅看体系认证，还会追问设计数据如何隔离、外发如何审批；出口管制环境下，数据跨境的合规口径也需要技术手段支撑。这些要求最终都指向同一个问题：能不能拿出一套持续运行、随时可查的管控记录。

从泄密的现实路径看，半导体行业的风险点集中在几类动作：把工程目录同步到个人网盘或私有代码仓库；通过即时通讯把版图截图、参数表发出去；外协与联合开发边界上账号权限模糊；离职前集中打包下载、改名分卷外发；以及用手机拍下屏幕上的关键图纸。这些动作单次看起来都不起眼，串联起来就是一条完整的泄露链路。对半导体企业而言，防泄密的重点不是发现「谁有问题」，而是让核心数据从技术上「带不走、看不懂、追得到」。

半导体核心数据资产的三点特征

特征	说明
单点价值极高	一套完整版图、一份工艺配方，背后是数亿元研发投入与多年经验沉淀，单个文件的价值远超普通商业文档
泄露不可逆	核心工艺参数与 IP 一旦流出无法召回，对手得到的不仅是数据，还有企业踩过的所有弯路
流转不可避免	流片、封测、授权、外协环环相扣，数据必须出手的场景多，靠封堵网络出口无法根治

半导体行业的数据防泄密不是给网络多加几道闸门，而是给数据本身加上一道「跟着文件走」的锁：文件在授信环境里照常使用，离开授信环境就失去价值，每一次外发、每一份副本都有审批和记录可依。本方案即围绕这一主线展开。

02 需求分析

结合芯片设计、晶圆制造、封装测试三类企业的典型环境，我们把数据防泄密的共性需求归纳为五个方面。它们彼此关联：数据以明文散落是起点，出口多而杂是路径，工具链敏感是约束，人员流动是高发期，举证能力是最终底线。

设计与工艺数据明文散落，密级边界靠制度维持

- RTL 代码、网表、版图、仿真波形、工艺配方、量测数据以明文形式分布在工程师工作目录与共享存储中，同一份数据往往存在多个副本，「哪个是受控版本」没有技术答案。
- 设计、工艺、测试部门之间频繁交换文件，一份 GDS 从设计端到制造端要经过多次复制，每个环节都可能留下不受控副本。

- 密级管理多靠目录命名与口头约定，低密级人员打开高密级文件没有任何技术障碍。

工具链高度敏感，安全机制不能拖慢产线与研发

- 设计端依赖 Linux 工作站、大内存计算服务器与 EDA 工具链，制造与封测端有 MES、SCADA 等产线系统配套终端，防泄密客户端必须兼容多类环境且不改变使用习惯。
- 编译、综合、仿真、DRC/LVS 都是长任务、高 IO 操作，加密若过度介入读写路径，直接后果是项目节点延后，团队会主动绕开安全机制。
- 产线终端对实时性要求苛刻，任何导致机台停机的安全策略都是不可接受的。

产业链交付出口多，每一环都需要「出去的那份可控」

- 流片交付：向代工厂提交 GDS/OASIS、DRC/LVS 报告，数据量大、通道多样（专线、FTP、移动介质）。
- 客户与授权交付：向潜在客户提供 IP 评估资料、向客户提供样片配套数据，既要给到够用的程度，又不能给全套。
- 外协协同：联合开发、IP 集成、第三方验证团队接入研发环境，数据边界最模糊。

人员流动是泄密高发期，缺少可预警的信号

- 离职前批量下载工程目录、集中压缩、分卷改名、上传个人存储，事后只能看到结果。
- 把代码片段发到技术社区求助、把工艺问题发到行业群里讨论，是工程师的常见习惯，对核心 IP 却是实质性外泄。
- 保密协议与竞业条款在举证时缺少技术侧记录支撑，追责难以落地。

审计与举证能力薄弱，客户审厂与内部追责都吃力

- 操作日志分散在文件服务器、版本库、网关等处，缺少按项目维度的统一检索。
- 被客户问到「这批数据被谁访问过、发给了谁」，往往需要数天人工排查，无法当场答复。
- 多站点运营下，总部与各基地策略不统一，IT 与信息安全团队人力有限，难以分头维护多套系统。

03 方案设计

半导体行业的数据防泄密，本质是三个问题：数据本身有没有锁、出去的那份可控不可控、事后能不能说清楚。因此方案不追求管控点的堆叠，而是围绕一条主线展开——让核心数据始终以密文形态受控流转，让每一次外发都有审批与痕迹，让全部操作可检索、可举证。

围绕这条主线，方案以「一个平台、三道防线」组织能力：

防线	能力	解决的问题	实际效果
防线 01	数据透明加密	带走也没用	文件在授信环境正常打开、编译、仿真，离开授信环境即为乱码
防线 02	受控外发与出口管控	出去的可管	外发走审批、限定条件、全程留痕；打印、截屏等出口叠加水印
防线 03	敏感识别与审计溯源	事后查得到	敏感数据有台账、行为有记录，审厂与追责拿得出证据

三条设计原则

- **按项目与环节分域、按密级授权**——以项目组、工艺环节作为隔离单元，一个团队一套安全域，密钥分级管理；低密级账号打不开高密级文件，跨域协作以授权代替解密。
- **透明、不改编程习惯**——加密在驱动层完成，保存即密文；EDA 命令行、编译脚本、MES 调用方式一律不改，安全机制对研发与产线「不可感知」。
- **性能与稳定优先，能灰度、能回退**——上线前对大文件顺序读写与海量小文件场景分别压测，形成性能基线；按项目组灰度推进，异常可单机回退，底线是不影响流片与产线节点。



实施路径：三步走

步骤	阶段	内容
第一步	单项目试点	选一个核心项目组先行部署，跑通加密、外发、审计三条主链路，同步完成性能基线测试
第二步	研发与产线域推广	覆盖设计、工艺、测试团队与产线配套终端，异地基地统一纳管，策略由总部集中下发
第三步	制度完善与常态运营	把策略与保密制度、客户审厂应答逐条对应，形成可季度复核的管理闭环

04 解决方案

方案能力围绕「数据加密防泄密」主线展开：从透明加密、工具链适配、受控外发、出口管控、敏感识别到审计溯源，六个动作串成数据从产生到归档的完整链路，全部能力共用一个客户端与一个管理平台。

1.1 核心数据透明加密

数据的价值在内容而非存放位置，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，离开授信环境打开即是乱码。加密不改变任何人的使用习惯，却让「拷一份带走」从技术上失效。

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
只读交付	提供给客户评估的 IP 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	代工厂回传数据、客户来图、外协交付件	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、已公开 datasheet	保持原有习惯，由外发审批与审计兜底

实施要点

- 按项目分配模式：核心项目组启用透明加密，读取型岗位用智能加密，对外评估件设为只读，外来交付件用落地加密。
- 国密算法与分级密钥：采用 SM3/SM4 等国密算法，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，也为客户审厂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、编译中间产物等经审批加入例外，避免误伤工具链。

1.2 半导体工具链与系统适配

安全方案如果让综合变慢、让仿真排队、让机台报警，一定活不过一个流片周期。因此第二个动作是把加密做进工具链的读写路径，而不是悬在系统外。

- Linux 环境支持：客户端支持主流 Linux 发行版与国产操作系统，命令行、脚本、调度系统的调用方式不变，不依赖图形界面。
- 共享存储适配：NFS 与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，不改变原有权限模型，跨站点挂载同样按策略生效。
- 产线系统兼容：MES 与机台配套终端单独分组、单独策略，保障实时任务不受影响。

1.3 供应链协同与受控外发

半导体产业链的分工决定了数据必须流动，管控的目标不是「不出去」，而是「出去的那一份可控」。所有外发统一走「申请、审批、受控、留痕」四步：

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 负责人分	超出预设范围自动升级，驳回须填原因

环节	动作	落地方式
	级审批	
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、禁止另存、叠加水印
留痕	记录谁、何时、发给谁	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受控通道，传输前后校验完整性，交付清单与审批单一一对应，杜绝「多交一层版图」这类事故。
- **IP 授权与客户评估**：评估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。
- **外协与联合开发**：为外协团队建立独立安全域，只开放其负责模块的目录授权，交付件以落地加密方式进入，项目结束即回收权限。

邮件通道对已备案的代工厂、封测厂与客户邮箱放行，其余外发一律审批；出差与现场支持可申请离网授权，到期自动失效。

1.4 数据出口管控与水印追溯

文件落到纸面、落到介质、落到屏幕之外，加密锁就不再起作用，因此对高频出口逐一设置策略，让每一次输出都带得上痕迹。

出口	主要风险	管控方式
移动介质拷贝	整目录打包带走	非授信介质拷出受控文件即阻断，授信介质内文件保持密文
打印	版图截图、测试报告外流	审批后输出、叠加水印、内容留存备查

出口	主要风险	管控方式
截屏与拍照	评审会上拍走关键图纸	截图管控，屏幕叠加姓名、工号、项目代号水印
剪贴板与拖拽	参数表、代码片段三秒搬走	受控内容禁止带入外部程序与网页

水印可追溯：纸面与屏幕统一叠加姓名、工号、项目代号与时间，文件流出后能锁定到人；**内容可复核**：打印不仅记录页数，还留存输出内容；分级豁免：公开资料不必层层审批，避免过度管控拖累效率。



1.5 敏感内容识别与分类分级

分类分级是加密策略的前提，落到执行层面要先回答三个问题：哪些文件含核心 IP，它们在哪台机器上，现在是不是明文。

环节	做什么	输出
01 扫描	扫描研发终端、共享存储与文件服务器	待检文件清单与分布
02 识别	关键词、正则、文件指纹多规则匹配	命中文件与置信度
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、阻断外发、纳入分级策略	处置结果与责任人

半导体行业常见敏感特征（规则库可按项目自定义）

芯片型号与项目代号命名规则、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 文件指纹、RTL 顶层模块名、DFT 向量、封装与 pinout 定义、尚未公开的 datasheet。

识别是起点，分级与策略才是终点：扫描结果要转化为「哪些目录必须加密、哪些岗位只能只读、哪些外发必须审批」的具体规则；同时避免过度管控，开源代码与公共库保持原样。

1.6 行为审计与追溯取证

防泄密的最后一环是「说得清楚」。审计的价值不在于记录了多少条日志，而在于需要的时候能当场还原整条事件链。

环节	内容
统一采集	文件操作、外发、打印、截屏、剪贴板、邮件、即时通讯等操作统一记录，断网缓存续传
聚合检索	按人、时间、项目、关键词、文件类型组合检索，从一条记录还原整条链路
输出取证	审计报表、事件链条、责任认定材料随时导出

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、打印。
- **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、高频使用截屏工具。

客户审厂或内部追责时，能当场调出记录、说清路径、指明责任人的团队，处理成本与只能回答「我们查一下」的团队完全不在一个量级。

05 方案优势

半导体企业选型时最关心的三个问题：会不会拖慢研发与产线、要不要改现有环境、出了事能不能拿出证据。对应的答案构成这套方案的基本盘。

优势	说明
透明加密：不动工具链	加密在驱动层完成，编译、仿真、EDA 与 MES 调用方式不变；Windows 与 Linux 同源客户端，性能有基线、可回退
数据自带锁：泄露即失效	核心数据以密文形态存储与流转，离开授信环境即为乱码，防护跟着文件走而不是跟着网络边界走
国密合规：对标体系要求	采用国密算法、密钥分级管理，访问控制与审计措施可映射等级保护与数据安全相关条款，客户审厂时拿得出技术口径
分域授权：贴合研发组织方式	以项目组与工艺环节划安全域，密钥分级、跨域越权在客户端侧即被拦截
闭环管理：事前事中事后	事前加密预防、事中外发审批与出口管控、事后审计取证，三段能力串成一条链
多站点统一纳管	总部与各设计中心、生产基地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
核心数据「可用不可带走」	设计与工艺数据在内部自由流转，离开授信环境即为乱码，加密不改变研发习惯，却让拷贝带离从技术上失效
外发「可管可控」	流片、授权、评估、外协四类交付全部走受控通道，出去的每一份都有审批、有限定、有水印
举证「拿得出」	日志、报表与事件链可当场调取，客户审厂、投资尽调、内部追责不再依赖人工翻查
研发「不降速」	性能有基线、策略可灰度、异常可回退，安全不以拖慢流片与产线节点为代价，制度才能长期运行
管理「从制度到机制」	把依赖保密协议与人盯人的管理方式，换成持续运行的技术机制，制度写在纸上，机制跑在数据上

这五条价值指向同一件事：让半导体企业的核心数据从创建、流转到归档的全生命周期都处于受控状态。对以技术与工艺立身的半导体企业而言，这既是竞争的护城河，也是面对监管与客户时最实在的底气。

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。



400-666-2563

www.wgj7.com

河北·石家庄

安企神软件®