

vinchin

筑牢集成电路数据安全底座

云祺制造、半导体灾备解决方案

主讲人：江苏售前吴昊良

目 录

PART 01 制造、半导体产线的数据安全挑战

PART 02 分级灾备的建设方法论

PART 03 云祺分级灾备方案解析

PART 04 部署场景、路径与价值

PART 01

制造、半导体产线的数据 安全挑战

先看清楚风险在哪、代价多大、合规底线是什么，再谈怎么防。

制造、半导体产线是“数据驱动”的连续生产系统

一座 12 英寸晶圆厂，从投片到出货经历数百道工序，由 MES 统一调度、EAP 直连机台自动执行。

生产过程 **不可随意暂停**：在制品晶圆对工序间隔时间敏感，系统中断直接威胁整批产品。

产线数据的三类核心资产

 **工艺配方 Recipe**
机台运行的核心参数，外泄或损坏即停产

 **生产数据（WIP / 批次追溯）**
在制品状态与追溯记录，丢失无法补录

 **良率与设备数据（YMS / FDC）**
工艺改进与客户交付的核心依据

晶圆厂核心 IT 系统全景

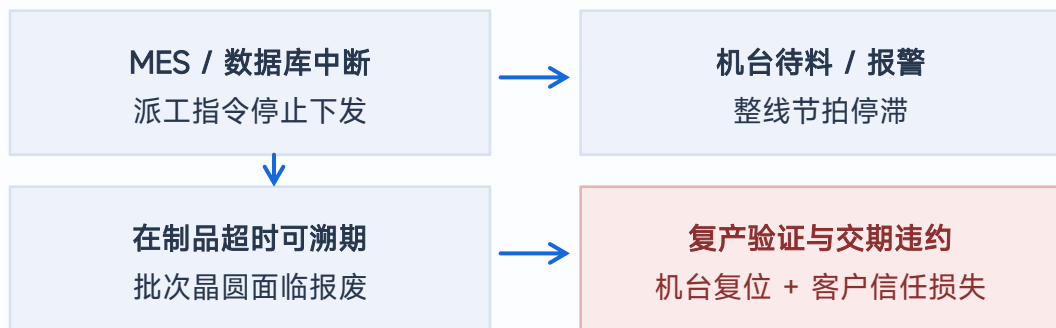


系统层层依赖：MES 中断 → EAP 停摆 → 机台待料。

任何一个环节的数据不可用，都会向上传导为整线停产。

非计划停机：损失不止在停机的每一分钟

一次系统中断的代价传导链



恢复系统只是第一步：机台需要复位校准、工艺需要重新验证、超期批次需要判定处置，实际复产时间往往是系统恢复时间的数倍。

数百万美元级

行业公开报道显示，晶圆厂任何非计划停机都可能造成数百万美元的损失

7 × 24 小时

产线全年连续运转，容灾系统不能依赖“停机维护窗口”完成备份与恢复

分钟级容忍

核心生产系统的可用性要求以分钟计，传统“天级恢复”的备份方式无法满足

产线数据安全的六类典型风险



勒索软件攻击

半导体已成勒索攻击重点目标，曾有头部企业因工业网络入侵导致整条 12 英寸产线瘫痪；备份数据本身也是攻击对象



电力与机房事件

市电闪断、UPS 切换失败、制冷异常，造成批量设备与系统同时下线



灾害级事件

火灾、水浸、地震导致机房整体损毁，本地备份与生产数据可能同时丢失



硬件与平台故障

服务器、存储、虚拟化平台宕机，承载其上的 MES / 数据库同步中断



人为误操作

误删数据、错误变更、Recipe 误修改，是产线数据丢失的高频原因



备份失效风险

“备份了但恢复不出来”：备份数据损坏、未被验证，关键时刻才发现不可用

结论：风险来源不同、影响等级不同，**用同一套备份策略覆盖全部系统，既防不住灾难，也浪费资源**——这正是“分级容灾”的出发点。

合规底线：数据备份已从“可选项”变为“必答题”



国家法律法规

《数据安全法》

要求建立数据安全管理制度，采取备份等措施保障数据安全

《网络安全法》

网络运营者须采取数据分类、重要数据备份和加密等措施



等级保护 2.0

第二级：要求提供数据本地备份与恢复功能

第三级：要求提供异地实时备份、重要数据处理系统热冗余

产线核心系统普遍按三级要求建设，**备份恢复能力需可验证、可审计**



客户与供应链审计

车规芯片、头部大客户普遍对代工厂开展供应链安全审计

批次追溯数据不可丢失、交付连续性有保障，是**承接订单的前置条件**

RTO / RPO 指标被写入越来越多的商务合同条款

容灾建设同时回答三个问题：**法律要求做到、等保测评通过、客户审计认可。**

PART 02

分级灾备的建设方法论

用 RTO / RPO 两个指标给系统定级，让每一分投入对应明确的恢复承诺。

为什么“一刀切”的备份不适合半导体产线

“一刀切”统一备份的三个困境

① 核心系统救不快

MES 与 OA 用同一策略：每天一次定时备份，MES 中断后要花数小时恢复，丢失一整天生产数据

② 一般系统浪费钱

为所有系统都上 CDP 与双活：邮件、文件服务器享受核心系统待遇，存储与授权成本成倍增加

③ 恢复顺序没章法

灾难发生时先恢复谁？没有定级就没有恢复优先级，现场全靠临时决策，RTO 不可控

分级容灾的核心逻辑

系统重要性 → 容灾等级

容灾等级 → 技术手段与投入

两个指标定等级

RTO 恢复时间目标：系统中断后，多久必须恢复运行

RPO 恢复点目标：最多允许丢失多长时间的数据

分级的三个收益

- 核心系统获得分钟级恢复能力，产线停机风险可控
- 一般系统用低成本手段覆盖，整体投入更经济
- 灾难预案自带恢复优先级，演练与实战有据可依

五步落地：从业务影响分析到持续演练

① BIA 影响分析

① BIA 业务影响分析（联合产线与IT）

盘点产线全部系统与数据资产，逐项评估：中断 10 分钟 / 1 小时 / 1 天分别带来什么后果，形成影响清单

② 系统定级

② 系统定级（RTO / RPO 双指标）

按影响清单确定每个系统的 RTO / RPO，归入 L0-L3 四个容灾等级，并明确恢复优先级顺序

③ 技术匹配

③ 技术匹配（等级对应手段）

L0 用 CDP 实时保护 + 容灾接管，L1 用定时备份 + 瞬时恢复，L2 用无代理备份 + 异地副本，L3 用归档

④ 策略配置

④ 策略配置（备份窗口避开高峰）

按等级配置备份频率、保留周期、传输限速与存储位置，策略与产线生产节拍错开，不影响生产性能

⑤ 演练验证

⑤ 演练验证（让指标可兑现）

定期在隔离环境做恢复演练，输出演练报告；验证不过的等级与策略回到第 ③ 步修正，形成持续闭环

四级容灾标准：每个等级都有明确的恢复承诺



容灾等级	等级定位	RTO 目标	RPO 目标	技术手段
L0 核心级	中断即停产的生产系统	分钟级	≈ 0	CDP 秒级实时备份 + 容灾接管（备机无缝接管业务）
L1 关键级	支撑生产的关键业务系统	≤ 30 分钟	≤ 15 分钟	高频定时备份 + 瞬时恢复（秒级拉起任意备份点）
L2 重要级	日常运营支撑系统	≤ 4 小时	≤ 4 小时	每日无代理备份 + 异地副本，防止站点级灾难
L3 一般级	历史数据与低频系统	≥ 24 小时	≥ 24 小时	周期备份 + 长期归档，满足追溯与审计保留要求

说明：RTO / RPO 目标值为行业通用分级参考口径，实际定级需结合各家工厂的产线节拍、批次周期与客户合同要求，在 BIA 阶段确定。

映射示例：晶圆厂系统该进哪个等级

L0 核心级	MES 生产执行 EAP 设备自动化 核心数据库（生产库） Recipe 管理	中断即全线待料停产，数据丢失即批次追溯断链，必须 RPO≈0
L1 关键级	YMS 良率管理 SPC 过程控制 FDC ERP WMS 仓储 质量管理体系	影响良率分析与物料供给，可容忍短时中断，但恢复必须快
L2 重要级	OA 邮件 文件服务器 研发文档 报表平台 测试环境	不直接影响产线节拍，但含经营数据与知识产权，需防站点 级灾难
L3 一般级	历史批次数据 设备历史日志 到期归档数据	低频访问，重点在长期保留、防篡改与可追溯

PART 03

云祺分级容灾解决方案解析

从总体架构开始，逐级看能力如何落到半导体产线的真实场景。

总体架构：一套系统覆盖 L0-L3 全部分级需求

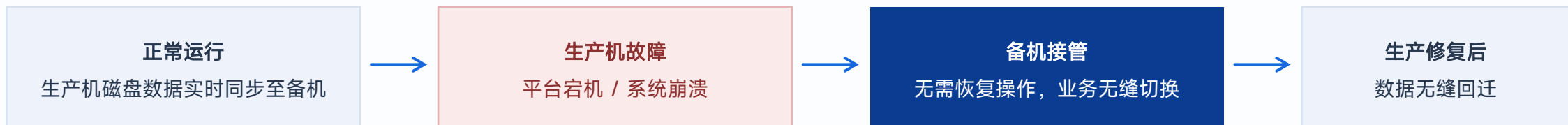


统一管理：一个 Web 控制台管理两地所有保护策略 | 架构遵循 3-2-1 备份原则：3 份数据、2 种介质、1 份异地

L0 保护：MES 中断，备机分钟级接管

适用对象：MES、EAP、核心生产数据库。云祺实时备份支持基于秒级磁盘卷整机 CDP 与应用一致性，配合容灾接管实现业务无缝切换。

故障发生时的接管过程



RPO ≈ 0

数据实时同步，故障点前的生产数据零丢失，批次追溯不断链

RTO 分钟级

接管模式下备机直接承载业务，相比恢复操作大幅缩短中断时间

应用一致性

数据库 CDP 到事务级粒度，保证 MES 数据库接管后状态一致可用

L1 保护：瞬时恢复，秒级拉起整机业务

适用对象：ERP、YMS、SPC、FDC、WMS 等。云祺可在秒级时间内恢复任意时间点的备份数据并立即启动虚拟机，恢复时间与备份数据容量无关。

一次 ERP 故障的两种恢复路径

传统整机恢复

数据拷贝回生产存储，数小时起，与容量成正比

云祺瞬时恢复

直接从备份存储启动虚拟机，秒级完成

瞬时恢复期间不改动原始备份数据；生产环境修复后，业务与数据可无缝回迁至生产平台。

配套能力：**细粒度恢复**——无需整机还原，即可秒级提取单个文件、单条日志，用于快速定位问题。

在产线里意味着什么

批次数据随时可回查

任意备份点均可秒级挂载，误删的批次记录、改错的 Recipe 立即找回

关键系统中断以分钟计

ERP、YMS 故障先在备份环境拉起服务，再择机回迁，业务不等数据搬迁

恢复时间可承诺

无关数据容量，恢复时间恒定，RTO 指标可以写进 SLA 并兑现

L2 保护：无代理备份，海量系统低运维覆盖



适用对象：OA、邮件、文件服务器、研发与测试环境。云祺为市场上 98% 的主流虚拟化平台提供无代理备份，无需在虚拟机内安装任何软件。

对比维度	传统有代理备份	云祺无代理备份
部署方式	每台虚拟机安装代理，逐台维护升级	输入平台账号即可接入，自动扫描全部虚拟机
运维成本	数百台虚拟机场景下管理成本高、兼容性风险大	运维成本降低数十倍，屏蔽虚拟机内部细节
生产影响	代理常驻占用虚拟机 CPU / 内存资源	直接与虚拟化平台交互，对生产系统近乎零侵入

备份效率的三项关键技术

永久增量 + CBT

首次全备后只传变化块，备份窗口与带宽占用大幅下降

重删与压缩

优化备份存储空间，降低海量副本的存储成本

多线程 + 限速

自定义线程数与限速策略，备份不挤占生产网络

海量小文件备份：产线最难啃的一块数据

vinchin

半导体产线的小文件从哪里来

- 机台运行日志、报警记录，每天持续产生
- AOI / 量测设备的检测图片与结果文件
- 工艺文档、研发图纸、Recipe 版本文件

单厂文件规模常达千万至亿级，多数文件只有 KB 级大小

传统备份的四个瓶颈

扫描慢：目录深且广，全量遍历耗时长

传输低效：逐个小文件网络交互，带宽空转

窗口超时：备份跑不完，挤占生产时段

恢复难找：从千万级文件中定位单个文件费时

云祺海量小文件专项技术



自适应扫描算法

按目录广度与深度动态调整遍历策略，提升发现效率



多线程 + 边扫边传

生产者-消费者模型，扫描与传输并行，不互相等待



小文件合并打包传输

自动合并为大对象传输，减少网络交互，带宽利用率提升



文件指纹增量比对

多维关键信息构建指纹，快速识别变化文件，增量精准高效



多节点横向扩展

文件目录按节点划分并行备份，性能随节点数线性扩展

NAS 免代理接入（NFS / CIFS 挂载，不装插件） | 恢复方式灵活：覆盖恢复 / 新建恢复 / 异机恢复 / 单文件精确查找 | 支持分时段限速与异地副本

广兼容 + 信创适配：与产线现有架构无缝共存



产线 IT 环境新旧并存、异构复杂。云祺与 100+ 厂商完成兼容适配，国产化替换过程中保护能力不中断。

环境层	国际主流环境	国产 / 信创环境
虚拟化 / 云平台	VMware、Hyper-V、Nutanix、Proxmox、oVirt 等 15+ 平台	华为 FusionCompute、深信服 HCI、H3C CAS/UIS、SmartX、云宏 CNware 等
数据库	Oracle、SQL Server、MySQL、SAP HANA	达梦、人大金仓等国产数据库
操作系统	Windows、Linux	麒麟、统信 UOS 等国产操作系统
云原生 / 其他	Kubernetes 容器应用、NAS 文件数据	私有云、公有云混合架构统一管理

 **X2X 跨平台迁移与恢复：**虚拟化、物理机、云平台之间任意互迁（V2V / P2V / V2P 等），自动完成格式转换与驱动匹配——产线从国外平台向国产平台演进时，备份数据可以直接在新平台恢复，迁移过程不丢保护。

3-2-1 备份原则的落地方式

3

至少 3 份
数据副本

2

存放于 2 种
不同介质

1

至少 1 份
异地保存

云祺**异地副本**功能：本地备份自动复制到异地灾备中心。生产数据与本地备份同时损毁时，仍可从异地副本恢复、重启业务。

复制任务支持断点续传与带宽限速，适配跨园区、跨城市的广域网链路。

半导体行业典型用法：总部园区与 fab 厂区互备，或自建灾备机房 + 云归档组合，满足等保三级“异地备份”要求。

L3 归档：为追溯与审计而设计

长周期保留

历史批次数据、设备日志按年保留，保留策略到期自动合并备份点，空间可控

归档位置灵活

支持归档至本地存储与云环境，冷热分层，低频数据不占高性能存储

客户审计直接可用

批次追溯链完整、归档数据可校验，面对车规与大客户审计时，证据随取随用

防勒索：备份数据是全网最后的防线

勒索攻击的逻辑是“先毁备份、再加密生产”。云祺以 3-2-1-1-0-0 安全策略构建备份数据的全生命周期安全闭环。

3 份副本 · 2 种介质 · 1 份异地 · 1 份不可变 · 0 验证无错 · 0 信任访问

事前预防

WORM 防篡改存储：备份数据写入后不可修改、不可删除，勒索软件无法加密备份
端到端加密：传输与存储全程加密，备份数据即使被拷走也无法读取

事中检测

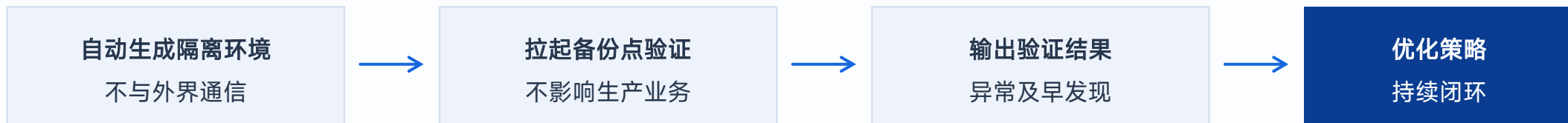
内置病毒查杀：备份过程中扫描数据，发现异常及时告警
内置防篡改驱动：实施严格访问控制，拒绝未授权程序访问备份数据

事后恢复

数据校验：恢复前校验备份数据完整性，确保“干净恢复”，不把病毒带回生产
瞬时恢复：生产系统被加密后，从干净的备份点秒级拉起业务，不付赎金也能复产

容灾演练：让“能恢复”成为可验证的事实

灾备系统最大的风险是“平时不演练，战时恢复不了”。云祺内置容灾演练平台，无需额外准备服务器、存储与网络资源。



对产线的实际价值



等保测评有证据

定期自动验证 + 演练记录，等保“备份恢复”条款直接举证



RTO 从纸面变成实测

演练中实测恢复时长，反向校准各等级的策略配置



团队真打仗时不慌：值班工程师按演练过的流程执行恢复，灾难现场不需要临时摸索；演练频率建议 L0 系统每季度一次、L1 每半年一次，与产线检修窗口同步安排。

集中运维：一个人管得住全厂数据保护

半导体厂 IT 团队普遍精简，容灾系统必须“配好策略就能自己跑”，把人力留给真正的异常处置。



统一 Web 控制台

两地三中心、多平台工作负载集中管理；备份操作四步完成：选对象、选存储、配策略、提交任务



报表与审计

备份成功率、容量趋势、恢复记录自动生成报表，管理层汇报与客户审计直接取数



告警通知

任务异常通过邮件、短信实时推送，与产线值班体系衔接，实现备份系统无人值守



分级权限

按角色分配管理权限，产线 IT、厂务、安全团队各司其职，操作留痕可审计

策略足够灵活，贴得上生产节拍

支持每日 / 每周 / 每月 / 滚动 / 一次性五种时间策略组合，备份频率可按 1-4 周间隔设置；备份任务可安排在产线低峰时段执行，配合传输限速，备份过程对生产网络与业务性能的影响可控。

PART 04

部署场景、建设路径与价值

一个典型部署场景、一条四阶段建设路径、一页价值总结。

典型部署场景：某晶圆制造企业分级容灾落地

场景（典型情况示意）

- 约 200 台虚拟机承载 MES / ERP / YMS 等系统，运行于国产超融合平台
- 核心生产库为 Oracle，另有达梦数据库承载新建系统
- NAS 保存设备日志与工艺文档，数据量约 80TB
- 总部园区建有灾备机房，与 fab 厂区同城光纤互联

分级策略配置

L0 MES + 生产库：CDP 实时备份，灾备机房备机接管

L1 ERP / YMS / FDC：每小时增量备份 + 瞬时恢复

L2 OA / 文件服务器：每日无代理备份 + 异地副本

L3 NAS 历史数据：每周备份 + 五年归档保留

全部备份启用 WORM 不可变存储与加密

部署拓扑

分厂区（生产中心）

超融合平台（200 VM）+ Oracle / 达梦数据库

云祺备份节点 + 本地备份存储（WORM）



同城光纤

CDP 同步 / 副本复制

总部园区（灾备中心）

容灾接管备机（MES / 生产库）

异地副本存储 + 归档存储

一套云祺系统统一管理两地策略；

生产侧无代理接入，不改动现有 IT 架构。

建设路径：四个阶段，先保核心再全面覆盖

第一阶段

评估与定级

约 2-4 周

- 系统与数据资产盘点
- BIA 业务影响分析
- 确定 L0-L3 分级清单

第二阶段

核心先行试点

约 2-4 周

- MES / 核心库 CDP 上线
- 本地备份存储部署
- 首次恢复演练验证

第三阶段

全面部署覆盖

约 4-8 周

- L1-L3 策略批量配置
- 异地副本与归档启用
- 防勒索策略全量开启

第四阶段

演练与持续运营

长期机制

- 定期演练与报告输出
- 策略随系统变更同步更新
- 配合等保测评与审计

实施三条原则

不停产实施：无代理接入 + 低峰窗口部署，建设过程不影响产线运行 | 先核心后一般：L0 优先见效，再扩大覆盖面 | 边建设边验证：每个阶段以恢复演练结果作为验收标准

价值总结：四个维度的确定收益



业务连续性

核心系统 RTO 从“小时级”进入“分钟级”，RPO 趋近于 0；产线中断风险从“不可控”变为“有承诺、可演练、可兑现”。



安全合规

防勒索闭环让备份数据自身安全可信；异地备份、定期演练、报表留痕，支撑等保测评与客户供应链审计。



投入更经济

分级配置避免“一刀切”的高成本；一套系统替代多套工具，无代理架构大幅降低长期运维人力。



自主可控

国产自研产品，全面适配国产芯片、操作系统、数据库与虚拟化平台，支撑产线信创演进的每一步。

THANKS



云祺公众号



云祺视频号