

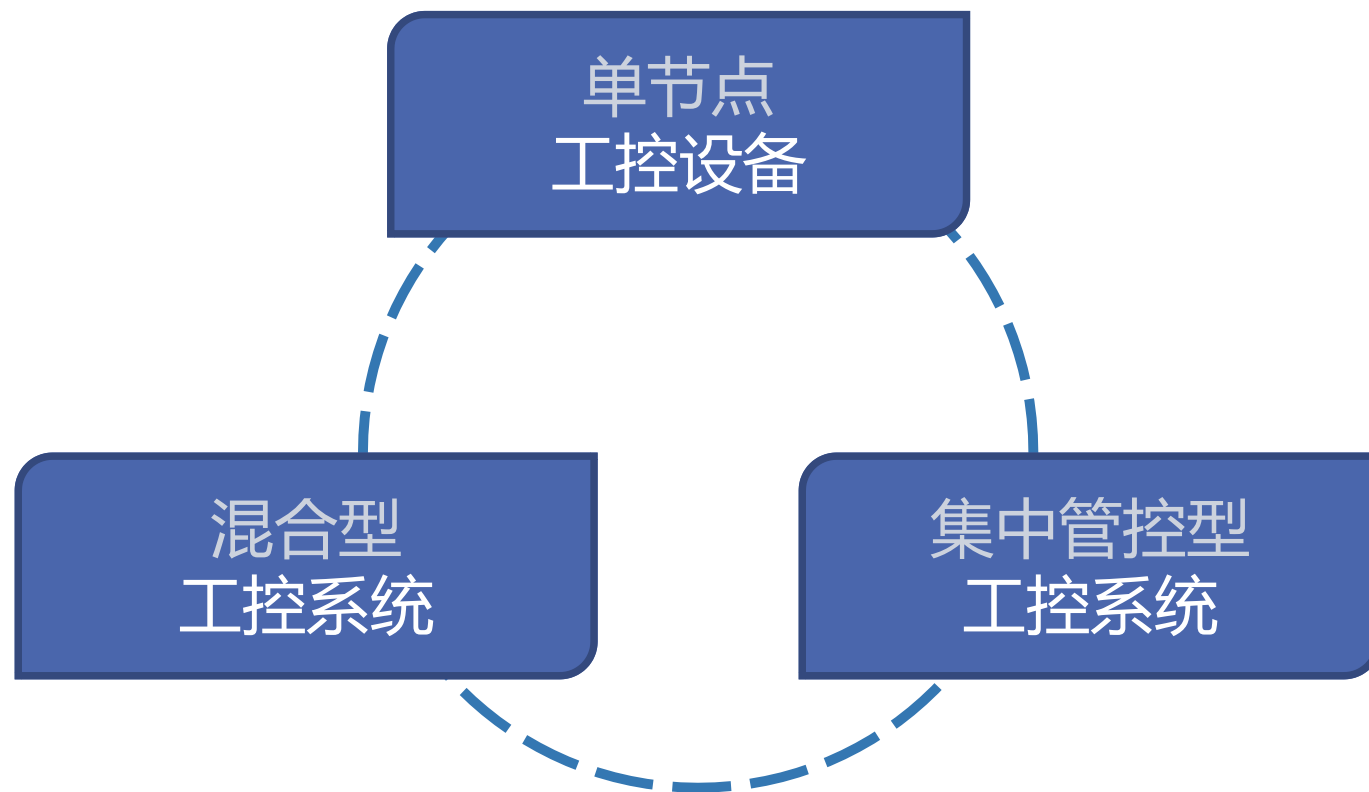
# 安克诺斯与制造业

——对工控机的保护

# 初识工控生产系统

工控机 ( Industrial Personal Computer , IPC ) 即工业控制计算机，与传统的办公用计算机不同，工控机采用专用的硬件设备，使用特殊的制造工艺而成。在控制现场、路桥控制收费系统、医疗仪器、环境保护监测、通讯保障、智能交通管控系统、楼宇监控安防、语音呼叫中心、排队机、POS柜台收银机、数控机床、加油机、金融信息处理、石化数据采集处理、物探、野外便携作业、环保、军工、电力、铁路、高速公路、航天、地铁、智能楼宇、户外广告等诸多领域得到广泛的应用。我们将从多个方面来认识工控机，以下将进行基础知识的介绍

# 一、应用架构与部署方式



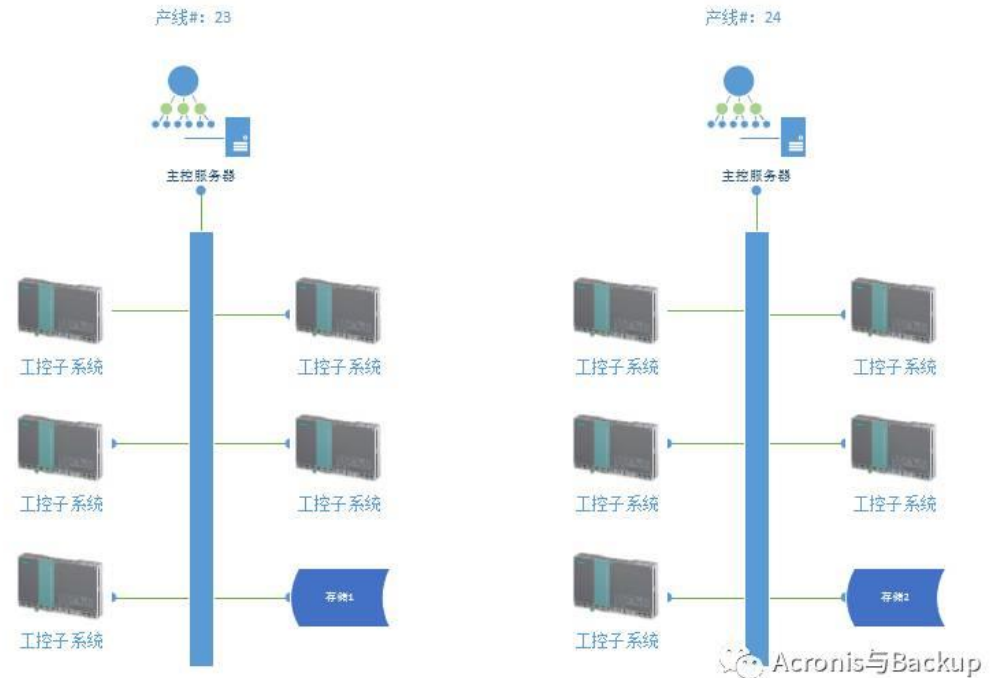
# 1、单节点工控设备

- 单节点工控设备只负责对单个生产环节进行控制，不与其它生产设备产生必然的数据联系。例如，某机械生产机床设备配置一台工控机，并在前端配置LED按键式控制面板，生产工人通过前端LED面板的操作对生产设备进行参数的配置与调整，最后生产出预期的产品。



## 2、集中管控型工控系统

- 集中管控型工控系统由一个主控端和多个子生产系统组成，主控端对子端工控机达到完全控制的目的。由主控端下发指令到子端，子端严格按主控端下发的指令进行操作，操作完成后产生的数据再反馈到主控端以达成数据的收集等目标。如上图所示，有两条生产线。



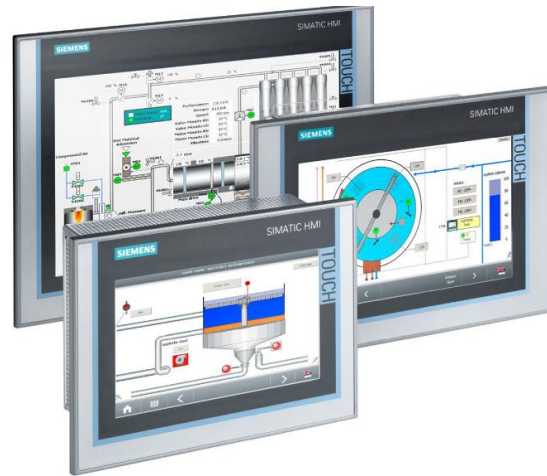
每条生产线都有一个主控端服务器对本产线的其它五个子节点进行完全控制。这类工控系统的应用非常广泛，例如生产型企业、气象采集与预报系统、银行ATM系统、交通调度系统等多节点联合工作的环境。

# 3、混合型工控系

- 混合型工控系统既可以完全集中式管控，同时每个子节点又可以独立操作。

## 二、硬件组成

- 工控系统与日常办公系统的硬件组成几乎相同，但是制造工艺不同。工控机的制造在对温度、湿度、防辐射、防粉尘、散热、防震动、防腐蚀等方面有严格的生产规格和工艺。因此，工控机的使用寿命相对于日常办公计算机会更长，更适合在恶劣的环境中运行。



# 通常工控机的硬件组成

- **主板**：工控机的主板与普通的计算机的主板从基础技术概念来看，几乎是相同的。同样为了更稳定的运行，所采用的是工业级的标准来生产制造。所以在稳定性方面有着很高的标准，同时定制化程度高。
- **CPU**：随着技术的发展与更新，目前大多数工控机采用的CPU与传统计算机的CPU的技术参数几乎相同。但是从工作环境来讲，工控机的CPU需要更好的散热，所以大部分的工控机会将常见的CPU散热风扇改成金属散热型设备。以占用更小的空间、更好的散热性、更稳定的运行。
- **内存**：与常见的内存没有本质的区别，但是在物理硬件的尺寸上设计更小化。
- **外存设备**：包括常见的模式硬盘、SSD硬盘、CF卡等。
- **输入、输出设备**：新型的输入、输出接口都采用USB接口，可连接常见的鼠标、键盘、USB存储设备、打印机等。
- **网络接口卡**：简称网卡，用于连接至网络。目前大部分的工控机所配置的网卡还是RJ45接口的网卡，很少有配置光纤接口的网卡。工控机不需要大量的数据传输，一般只配置RJ45接口的网卡。



# 三、工控机操作系统

工控机的操作系统从产品提供商来分，分为Linux、Windows、Unix等三大类，目前主流的操作系统是Windows。

从类型来分，可分为常规、嵌入式两类。两种类型的操作系统均有应用。

从版本来分，又分为服务器类操作系统和 workstation 类操作系统。大概整理如下：

- Windows XP
- Windows XP Embedded
- Windows 7
- Windows 7 Embedded
- Windows server 2003
- Windows server 2008
- Windows server Embedded

# 工控机应用程序

- 各类工控机的不同，所研发和采用的应用程序也不尽相同。此处对应用程序不做过多的讲述。下面的图片都可以称为是工控系统：



# 工控机数据与系统保护分析

# 一、数据VS系统，哪个更重要？

- 数据，还是系统，主要是和办公系统作对比。办公系统里，各类数据对组织机构的运营非常重要，例如我们常见的OA、CRM、ERP、邮件等。当然，这样聊天并不是说系统不重要，而是数据与系统同等重要。在某些方面，数据可能比系统更重要。**而工控机最重要的是系统和应用程序能够正常工作，那么生产就不会中断。**
- 因此，从这个角度来看，工控系统一定会比数据（此处所讲述的数据是指由操作系统或者应用程序所产生的数据，例如日志文件、生产过程中所产生的其它历史数据等）重要。因为从数据的组成来看，数据其实对工控机的影响很小，数据的丢失可能会影响到历史数据的二次使用等问题。但是如果操作系统或者应用程序出现问题导致生产受到影响，问题就非常严重了。试想，一个生产节点或者一条生产线，因为工控机的宕机而导致不能继续生产，那就会影响到整体公司或者项目的运营。例如生产型企业不能继续生产产品、银行ATM不能继续提供现金交易、监控系统不能及时获取影像资料、气象监控系统不能及时获取气象数据等。

## 二、硬件容易损坏

- 工控机的运行环境往往相对恶劣，对于硬件的损耗很严重。特别是对于外置存储设备，例如磁盘、FT卡等。如果这类存储设备损坏，将直接影响生产。例如磁盘损坏，生产系统宕机。需要产线维护工程师重新置换新的磁盘后，再部署操作系统、安装应用程序、配置应用程序等一系列复杂的操作。整个RTO周期非常长，严重影响生产效率。

# 三、工控机应用程序复杂

- 工控机所携带的应用程序往往由工控机的产品提供商提供，应用程序不常见，切极为复杂。一旦出现由软、硬件问题所引起的宕机出现后，用户方并不熟悉应用程序的再次部署。这将会导致生产中断。

## 四、昂贵的费用

- 首先是工控机，这类设备往往价格昂贵。用户大都不会置备一台冷备机作为灾难接管的策略。其次是产品提供方的上门服务费用，如果需要原厂技术人员上门提供技术支持服务，需要与厂商协调时间、协调人员等一系列流程，这一定对生产有严重的滞后，而且用户需要更多的时间成本和金钱成本。例如，需要某些产品提供商提供上门服务时，厂商的工程师从出家门的那一时刻起就会收取售后费用了。

# 五、对用户的哪些方面会影响

先说钱的事

工控机宕机，就表示不能再生产产品了。不论这个产品是一辆汽车、一个娃娃、一个监控数据等等。没有产品下线，就表示不能把商品卖到用户手里，就等于没钱赚了.....

再说钱的事

产线停线了，但是员工的工资、福利还要照常给大家的吧。

还说说钱的事

上面说了，工控机最容易坏的就是硬盘。大家都同意吧？没关系了，反正我从客户了解到的情况就是硬盘容易坏。那么硬盘坏了，你选择买硬盘还是买个整机回来？又是一笔开销啊.....别说花钱的事了，想想我就害怕！



## 最后一次谈钱

上面又说了，工控这东西复杂的很，没几个人能懂，万一出了问题，估计得找厂商或者产品供应商的工程师过来解决。这批人，往往上门都是要收费的，而且还不便宜。算法更神奇，基本原则是，从离开家门开始计费，直到问题解决回到家门停止计费。每小时少则几十美刀，多则几百美刀。一个问题解决下来，没个大几万搞不定。哎……想想就肉疼！

## 企业形象的影响

想像一下：  
原定一个月可以取车的，结果用户等了3个月；  
本来应该在高速收费站1分钟的事，结果排起了长龙；  
本来应该在附近的ATM机就可以取现的，结果跑了三站地；  
本来可以在附近就能给汽车加油的，结果跑出去10公里。

如果是我，  
我换一个汽车品牌；  
高速。。。算了这个忍了，准备好塑料带就好；

ATM，我换个银行；

加油站，我换个石化公司；

我换换换！！！！

# 常见的工控机保护方案

# 一、冷备机

- 冷备机是最有效的解决方案之一，能够在线上工控机宕机后，快速更换后达到生产中断最小化的目标。但是此方案也有不足：
  - 首先是代价高，用户需要单独购买冷备机，这对于用户来说可能是一笔不小的投资。
  - 其次是灵活性差，冷备机的应用程序的配置可能与宕机的工控机参数不匹配。需要时间来调整工控机的工作参数以达到与生产相匹配。另外还有存在风险，例如参数配置错误导致生产的产品不合格。
  - 冷备机方案，只适用于小面积使用。例如特别重要的工控系统，每年需要有99.99%的运行时间保证的。

## 二、磁盘陈列技术

- 在工控领域，为了防止系统宕机，在磁盘保护技术上，使用Raid-1技术做磁盘镜像来保证系统安全，将宕机风险降至最低。
- **先聊聊优点**：这种技术的使用，将系统宕机的机率降到了最低状态，Raid组中的任何一块磁盘坏了，系统都可以正常运行，除非所有磁盘都损坏。为什么说任何一块出问题呢，因为工控机本来体积就小，两块盘组一个Raid-1是最常用的方式。
- **缺点也很明显**，包括成本和系统宕机风险两方面
  1. 成本方面，每台都要增加一块硬盘，如果有成百上千的工控机，那么整体成本投入金额就会很大了。再者，硬盘本身是消耗品，有自己的生命周期，超过生命周期就要定期的替换了，这方面的成本也很高。
  2. 再说宕机风险，一台工控的Raid-1组发生两块硬盘同时损坏的可能性很低，但是还是有概率的。万一不幸中奖，后果可能很严重。
- Raid方式的保护方案，同样适用于对宕机时间特别敏感的用户使用。例如一些特定的监控及数据采集工控类应用等。

# 三、免费的Ghost方案

- 此方案在很多用户中得到应用，最大的优点就是免费，适用于小规模、对工控停机时间不太敏感的用户群体。不过有句话目前很流行，是这样说的：**免费的东西往往是最贵的**
- 但是这种方案有先天的不足。
- Ghost方案有产品的兼容列表，超出列表的操作系统是不支持的。换句话说，不兼容的操作系统就没办法去做镜像。
- Ghost需要关机制作镜像，在制作操作系统镜像时，需要将目标工控机关机后操作，这会影响到生产。
- Ghost在异构硬件平台，无法恢复镜像。例如将系统从一个型号的硬件迁移至另一个型号的硬件平台上。
- 最重要的一个，没技术支持。有问题自己处理，处理不了，就等着被处理。

## 四、磁盘克隆

- 所谓磁盘克隆就是将现工控机的磁盘使用工具软件克隆到另一个磁盘上，当出现磁盘损坏时快速更换磁盘以达到将RTO时间尽量缩短的目标。磁盘克隆虽然可减小RTO值，但是需要对源工控机关机才可以进行克隆，同样会影响生产。同样，磁盘克隆技术不能异构环境中使用。例如将现在磁盘在其它硬件平台上使用。

# 理想的工控机保护方案



# 1、工控机需要备份什么

- 关于这个话题，理想的解决方案是所有的数据尽在备份中。如果一定要区分，那么一定是可用的系统优于实体数据。就像我们前面提到的，可用的系统才是工控机最重要的。
- 所以，在对工控机的备份方案中，要将整个磁盘都置于备份计划中。所谓整个磁盘，除我们日常所见的类似C盘、D盘等卷外，还应该包含系统的MBR。所以磁盘镜像技术是最适合工控机的备份方案。以下所有话题均在使用磁盘镜像备份的基础上进行。

## 2、在线热备份方式

- 为了保障生产不中断，所提供的备份方案应该使用在线备份方式，既不停机在线备份。这种备份方式最大化的降低工控机的停机时间，不影响现在生产任务。

# 3、多种备份机制

- 可提供热备份、冷备份两种备份机制，在不可预期的环境中，可备份所有的兼容或不兼容的所有业务系统。包含Windows、Linux、 Unix等。

# 4、系统快速恢复

- 当系统出现宕机事件后，需要快速的恢复系统到可工作状态，无论是操作系统、应用程序、或者是硬件所引起的宕机。
- 操作系统或者应用程序引起的宕机时，快速使用可引导媒体进入工控机，然后将已存在的备份存档恢复至当前工控机。这样的恢复可将业务连续性保持最高状态，有效降低RTO时间。
- 由硬件引发的宕机，分两种情况。一种情况是非存储设备，例如内存、主板等硬件损坏。这种情况下只需要更换新的硬件既可，但这需要用户的足够可用的备件。另一种情况是存储设备损坏，例如磁盘损坏。此类情况只需要更换新的磁盘后，使用可引导媒体将原备份存档恢复至新的磁盘。

# 5、异机还原与系统迁移

- 工控机的软、硬件也是有生命周期的，在生命周期结束后有能力将现有工控机的系统整体迁移至新的硬件平台。降低迁移的时间、资金成本。同时，对于损坏的工控机，有能力将现有系统通过异机还原能力，迁移至新的硬件平台，保障业务连续性最大化，RTO参数最小化。

# Acronis工控机方案分析

一看标题是不是有点蒙圈？Acronis不是个备份软件嘛，能做备份，能恢复。

Acronis可以将工控系统的RTO时间缩短至2分钟以内。

怎么做到的呢？

这要归功于Acronis的Anydata引擎。Acronis最厉害的就是磁盘镜像，而且目前在业界还没有哪家的技术可以与之比拟。

啥叫磁盘镜像？

说简单点就是整个磁盘的所有的所有全部打包成一个文件。

# 1、让RTO等于0

- 这种方式对于RTO时间的要求非常严格的用户非常适用。说到RTO为0，其实只是理论说法。也就是从Acronis的角度来考虑的。从用户的角度来看，这个时间基本可以控制在2分钟以内。





## 这种方式的流程如下：

1. **备份**：采用热备份方式，先将整个工控的磁盘镜像出来。注意在备份的时候，一定是工控机运行正常的时候。这叫积谷防饥。
2. **恢复**：这里所说的恢复，并不是恢复到原机上，而是恢复到一块新的备用硬盘上。恢复完成后，作为备件存放。在这里可能有人会有疑问，恢复到新的硬盘上，这个怎么操作呢。其实很简单了。操作如下：
  - 在一台空闲的计算机上安装Acronis的代理程序，并将备份存档存放在此计算机上。
  - 计算机外接一个USB转换SATA、IDE的转换器
  - 将新的可用硬盘外接至此转换器上
  - 运行Acronis的恢复操作，将备份恢复至新的硬盘上。

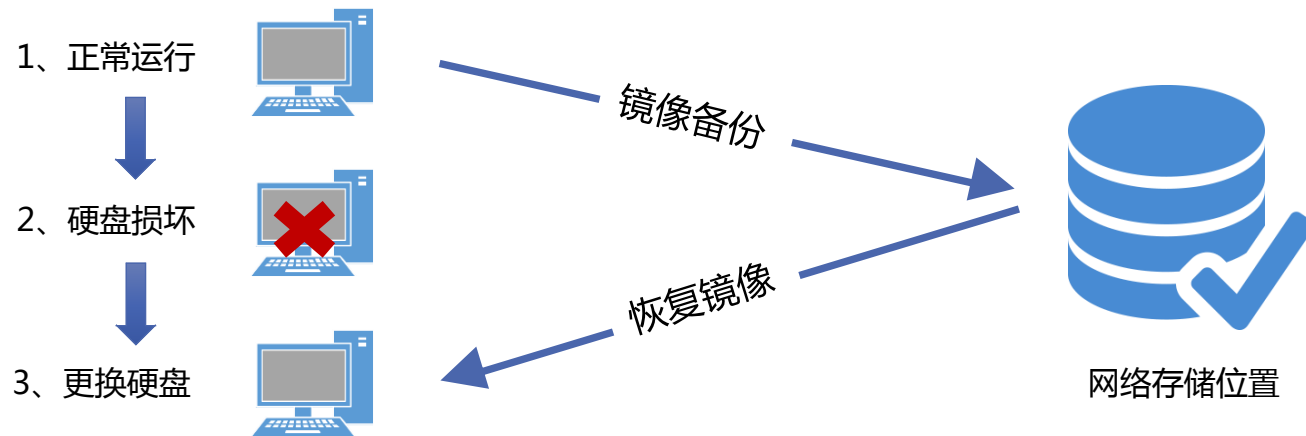


3. **接管**：当工控机硬盘损坏时，关机更换步骤2中的备份硬盘，更换完成后开机进入工作模式。

Over，大家可以算一下这样的灾难接管时间大概是多长时间。基本上两分钟内可以搞定吧，一分钟更换硬盘，一分钟开机时间。

## 2、让RTO时间=网络传输速度+磁盘性能

- 这种系统灾难拯救方式是通过网络方式，而非本地方式恢复。当工控硬盘损坏，更换新的硬盘后从网络引导，然后从网络存储位置将原备份存档恢复至本地新硬盘上。恢复完成后，重启工控机进入正常工产模式。架构示意如下图：



- 这种方式的系统灾难恢复，需要考虑网络带宽和磁盘性能。因为这两个参数决定了系统恢复的速度，也就是RTO时间。

# Acronis方案优缺点分析

# 1、在线热备份，无停机时间

- Acronis的磁盘镜像备份，使用在线备份方式，既热备份方式。也就是说，工控机该生产生产，该干嘛干嘛。Acronis在后台就把系统给备份了。方案相比Ghost、磁盘克隆等方式，节省了不必要的停机时间。

## 2、生产快速恢复

- 除了冷备机、Raid方案后，在软件解决方案方面还没有听说或遇到过比Acronis的这种系统恢复方式更快的。2分钟的RTO时间非常适合广大的制造生产型用户群体。这部分用户中，大部分都接受的宕机时间半小时左右。而Acronis的2分钟方案绝对称得上飞一般的速度了。有人会问了，能不能将RTO时间降到0？可以，只要你能把换硬盘的时间降到0，Acronis就可以！

### 3、更经济、更有效

- 所谓经济性更好，大家可以算一笔账就清楚了。例如：停机1小时不能生产，对生产的影响折合现金是多少；停止生产所造成的间接成本是多少，包括人力成本、资源占用等方面；恢复系统需要花费的成本等。这其实是一笔非常可观的成本额。而采购Acronis软件许可所需要的投资与上述加减法，很容易的得到了成本方面的投资占比。所以，Acronis的方案更具经济性，且安全有效。

## 4、缺点：花钱

- 买软件要花钱，老板不批很麻烦！

**其实，花小钱办大事！**