

# 信息技术 (IT)



# 运营技术 (OT)



## IT/OT 融合

推动全数字化制造业蓬勃发展

# IT/OT 融合

推动全数字化制造业蓬勃发展



过去，在工业制造企业中，信息技术 (IT) 部门和运营技术 (OT/运营) 部门可以相互独立，平行运作：运营部门负责维持工厂平稳运行，IT 部门则负责管理前台的业务应用。

两个团队偶尔也会通过协作成功开展一些项目（例如在工厂车间部署打印机或维护工业计算机），遗憾的是，这种良性合作机会十分罕见。大多数情况下，IT 和运营开展协作是因为出现了问题，而不是遇到良机。此类问题包括安全事件、系统故障和意外停机等等。无论是哪种情况，都基本不会在两个团队之间培养信任和协作精神。

但是，制造业正在发生改变。为了与时俱进，IT/运营的关系也必须随之改变。

有研究表明，企业高管对于其业内业外的成熟公司和创业公司表现出同等的担忧，因为这些公司部署的新技术和业务模式将对他们的市场地位产生不利影响。

为应对这种潜在冲击，各制造企业正致力于调整其流程、技术和业务模式。最有远见的企业不会仅止步于在这些变化中求得生存。而是努力成为变革的引导者，并进而获得竞争优势，提高运营效率，同时最大限度提高盈利能力。他们将引领制造业的全数字化业务转型。

显然，这一转变将给该行业的 IT 和运营专业人员带来全新且具有挑战性的课题。而最有经验的 IT 和运营领导者深知，要在这种新趋势下取得成功，必须开展更紧密的合作。

“全球全数字化业务转型中心表示，制造业是最易出现业务中断的 10 大行业之一”<sup>1</sup>。

1. [http://www.imd.org/uupload/IMD.WebSite/DBT/Digital\\_Vortex\\_06182015.pdf](http://www.imd.org/uupload/IMD.WebSite/DBT/Digital_Vortex_06182015.pdf)

有远见的运营领导者认为，他们用来支持实时决策的大规模运营数据可以为公司创造额外的价值。但是，他们需要 IT 同事的技术支持才能使数据富有意义，并提供给整个组织访问使用。此外，IT 同事还可以帮助他们更好地利用企业系统，例如企业资源规划 (ERP) 工具和制造执行系统 (MES)。

另一方面，IT 团队希望实现互联工厂的愿景并发挥其潜力（从改善供应链，到推动创新和最大限度减少停机）。但是，要实现这个目标，他们需要运营专业人员提供知识和技术支持，因为后者了解设备，并拥有设备的控制权。

两个团队都大致设想了他们的努力将会如何加强其公司和行业的未来发展，但是要充分利用此机会，双方必须开展协作。

这就是为什么过去安全和以太网项目通常特有的强制型 IT/OT 交互被更强大的合作联盟所代替。同时，IT 和运营团队所做的并不仅仅是对问题作出响应，而是在其公司的转型过程中发挥关键作用，帮助公司抓住新商机，实现竞争力，效率和安全性提升。

## 在本文中，我们将深入了解 IT/OT 融合推动实现全数字化制造转型的主要方式，包括：

01. | 通过雾计算支持实时决策
02. | 通过预测性维护消除意外停机
03. | 在工厂车间部署无线技术
04. | 在设备实现互联的新世界确保网络安全

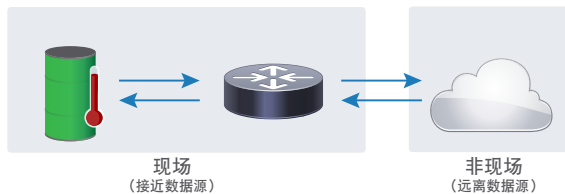
## 01. 通过雾计算支持实时决策

工业物联网的出现使得制造商收集的数据比以往任何时候都多。然而，这些数据具有多少价值，则取决于它们所能支持的决策。

正因为如此，仅依靠传统的云计算并非总能为制造业提供最佳解决方案。对时间极为敏感的决策应该更加贴近生成并使用数据的事物，以尽可能降低延迟并解决潜在问题。

多年来，制造商一直依靠监控和数据采集 (SCADA) 系统来实现实时决策。但是，这些系统通常不支持智能制造领域可望实现的企业级数据共享。

这就是为什么运营团队转向雾计算的原因，运营可通过雾计算实时访问工厂级任务关键型数据，同时将该知识在整个企业共享。这有助于实现快速决策，进而增强安全性并防止成本高昂的停机，同时可在不同地理位置的工厂之间实现信息共享，帮助运营领导者发现有益于安全和运营效率的企业级趋势。



值得高兴的是，IT 和运营一样喜欢雾计算。有了雾计算，IT 可实现真正的数据分类：

- 时间敏感型数据可在最靠近数据生成设备的雾节点上进行分析。
- 可等待数秒或数分钟的数据可传送到随时密切关注运营数据的一个中间节点。
- 时间敏感性最低的数据发送到云进行历史分析和存储。

此方法可节省带宽，优化数据中心资源的使用时机和使用方式。这有助于创建可扩展性更强的系统，为支持大量新型全数字化设备以及应对工厂车间的复杂性问题预留空间。此外，由于此方法还实现了在源头分析敏感数据，所以整个系统的安全性将得到提升。

### 客户案例：Mazak

[Mazak 需要一种基于标准的通用方法，以保护机床连接的安全性，并利用机床中丰富的原始数据创造价值。](#)适用于 IT 和运营技术 (OT) 的高级安全系统对防御内部和外部攻击者不可或缺。该应用需要在工厂车间的网络基础设施上运行，以便能够立即转化流程、设备综合效率 (OEE) 和传感器数据。该雾应用需要支持 MTConnect 规范，以便与现有系统和传感器集成。他们还需要实时分析功能来处理高频率振动、温度、冷却剂和声音输入，以便向操作员发出操作通知，并推动业务支持系统顺利工作。

他们实施了物联网连接（思科® 工业以太网 4000 交换机）、一个新应用框架（思科 IOx）、一个雾应用 (MTConnect) 和实时分析解决方案（思科连接流分析）。

业务成果包括：

- 利用 Mazak SmartBox Connected Machine 服务拓展了市场
- 通过在物联网网络基础设施上运行雾应用和实时分析，实现了成本整合
- 通过一系列可衡量的成果加快了价值实现，包括提高 OEE、提供持续性客户服务，以及提高机床利用率

[→ 了解详情](#)



## 02. 通过预测性维护消除意外停机

IT/OT 融合也在推动工厂维护模式发生转变。

大多数制造企业目前还在采用预防性维护策略。运营团队定期进行预防性维护以降低设备发生故障的可能性。此方法要求工厂维护其资产数据库，跟踪资产情况，并根据制造商的建议确定维护时间和维护方式。

虽然进行预防性维护明显好于在某个零件出现问题时才进行维护，但并非无可挑剔。这些方法很耗时、成本高且并不适用所有特定条件。由于维护计划基于最佳实践，并非来自维修设备的实际数据，这种方法几乎不可避免地会导致一定数量的意外停机和资源浪费。

当今世界，意外停机完全不可接受。在大多数制造环境中，利润率已经很低。任何与意外停机相关的成本（从生产损失到废弃材料和更换零件）都在打破盈利与亏损之间的微妙平衡。

这意味着减少意外停机是企业的当务之急。

不同于预防性维护程序，预测性维护技术使制造商可从实际受影响的设备收集实时数据，监控可能表明存在潜在设备故障的所有情况，然后在计划停机期间安排维护，这样也延长了设备的使用寿命并将显著降低维修成本。这些系统使用的是来自工厂车间的实际数据情报，而不是预估或最佳猜测。

转变为预测性维护方法可显著提高正常运行时间，而且这种方法可由 IT/OT 融合提供支持。运营部门可以通过从 PLC、设备和传感器收集关键数据来履行其职责，IT 部门则能够提供数据分析以及为数据赋予含义的其他工具。通过采用全数字化的维护过程，IT/OT 团队可以预测任何特定设备可能发生故障的时间，并相应地采取行动。

“ISA 数据显示，全球制造商每年因停机遭受的亏损总额约为 6470 亿美元。<sup>2</sup>”

### 客户案例：FANUC

[FANUC 是一家全球领先的数控机床系统与工业机器人公司，主要业务是向制造商提供设备。FANUC 使用大数据分析来确定可以防止故障发生的维护程序。](#)

凭借 FANUC 零停机解决方案，管理员可通过思科网络连接至工厂的思科边缘数据收集服务器，从而达到访问机器人运行数据的目的。

相关数据将被安全地传输至思科云，FANUC 的分析工具将在思科云中捕获“超出范围”的异常并判断是否需要提前维护。

然后，云应用会向 FANUC 维修人员和制造客户发送警报，告知是否需要维修。所需零件将被及时运抵工厂，以用于下次已安排的计划维修。

FANUC 美国的首席执行官 Rick Schneider 表示：“防止意外停机将为我们的客户节省很大一笔开支，并为搭载 ZDT 的 FANUC 机器人赋予极大的价值。我们将通过思科来帮助我们的客户获取这一新价值，并重新构想我们售后服务和技术支持的市场进入战略”。

思科/SCM World 调查项目的调查显示，制造商有望通过这些解决方案减少 48% 的意外停机。FANUC 案例表明，这个解决方案可以减少甚至消灭计划外停机。

[→ 了解详情](#)

2. <https://www.isa.org/standards-publications/isa-publications/intech-magazine/2013/feb/automation-it-predictive-maintenance-embraces-analytics/>

## 03. 在工厂车间部署无线技术



难以想象一个智能工厂没有采用无线技术会是怎样。有了无线技术，大量的设备、传感器和 PLC 以及与之一起运行的分析平台和辅助技术都将变得高效和实用。

但是，直到现在，在工厂车间中进行无线部署也并非总是可行选项。

工业环境变化极大，从充满挑战的建筑布局到恶劣的环境条件，例如灰尘、高温、高湿和振动。工厂经理也质疑无线技术能否支持任务关键型应用所需的设备数量、带宽、延迟水平和安全性。工厂为此会在厂区布设总计长达数英里的线缆，这样做既费钱，又费时。

但是，过去几年无线技术实现了飞跃。网络弹性的提升使得无线技术对工业环境来说比以往更加经济和实用。部署也会更快。

无线技术将为所有工厂带来变革。其将为远程监控、装配线转换和质量或供应链计划带来更大的灵活性和适应性。同时，它还将节省大量的成本。根据 Control Engineering，“无线方案比有线方案的成本低十倍，而且更灵活、更易于移动，需要更少的维护和修理。”<sup>3</sup>

IT 和运营可共同协作以在工厂车间成功部署无线技术，两个团队均可从中受益。IT 想要节省成本，减少故障排除，并且增加带宽，而运营团队则希望获得更多的敏捷性、提升质量和减少停机时间。

### 客户案例：戴姆勒

[对戴姆勒卡车北美公司 \(DTNA\) 而言，成功不仅仅意味着控制成本，而且关系着如何打造一间灵活的公司，以确保在当前和未来都能准确满足市场需求。其卡车品牌 Western Star 根据每个客户的需求进行定制，但是，这种程度的定制在大规模生产环境中存在后勤挑战。](#)

DTNA 决定，无论现在还是未来，它均需升级其美国俄勒冈州波特兰市生产基地的 Western Star 网络，以更好地协调定制和支持灵活高效的运营。

DTNA 选择了思科和 Rockwell Automation 作为战略合作伙伴，设计和部署基于融合全厂以太网 (CPwE) 验证设计指南的新网络。Cisco Aironet<sup>®</sup> 无线接入点为整个工厂提供安全可靠的 Wi-Fi 连接。团队领导和主管可以通过无线电话进行可靠的通信以管理车间的生产。无线设备，例如 iPad，可以用来实时确认卡车配置、检查零件供应水平、从该仓库检索零件和确认卡车状态。

通过在安全、易管理和融合的环境中安装 IT 和自动化网络，DTNA 经理可获得整个流程的实时可视性。数据将被安全地传送给经理，帮助他们做出更好、更快的决策以维持工厂的高效运行。当设备需要维护或维修时，软件定义网络 (SDN) 还支持远程故障排除以将停机时间降至最低。

该联合架构可扩展为任何规模或配置，DTNA 可将 Western Star 工厂用作模板，并在其他工厂进行部署。

### → 了解详情

3. <http://www.controleng.com/channels/manufacturing-it/case-studies/single-article/outstanding-industrial-wireless/4671e1ff860b0b2167e5b73b08a0c819.html>

## 04. 在设备实现互联的新世界确保网络安全

网络安全对制造企业来说非常关键。保护知识产权和客户信息对公司的长期运营和企业信誉至关重要。同时，遭到破坏的生产系统可能影响质量、盈利能力，甚至生产安全。

就在不久之前，大部分制造企业的经理们还不担心生产设备的安全，因为这些专业设备还没有和企业网络连接。然而将设备联网带来的好处也显而易见，例如，收集的数据可用于分析以减少停机时间，提高运营效率，并改善安全性和提升产品质量。但是，这一新变革以及网络安全威胁的增加，使得我们需要一个确保安全的新方法，再也不能依靠隐藏获得安全的传统策略了。

现在的解决方案不但要能连接网络，还要能够监控并确保数据安全。方案既可以部署在现今的网络环境中，也能在遗留设备上运行。而且方案还必须提供深度防御功能，以组织、强化、防御和应对威胁。

在制造业中实施此新网络安全方法需要 IT 和运营团队相互协作。IT 能深刻理解网络安全协议和策略，拥有管理实施和确保合规性的经验。

运营团队在落实网络安全工作中，也起着至关重要的作用。例如，一种能有效确保网络安全的方法通常需要定期进行系统更新，但是，在没有咨询运营团队的情况下进行部署将会面临潜在的停机灾难。运营团队必须参与决定部署更新升级的时机，并评估所有对生产系统的潜在影响，理想的部署时机是设备进行计划内维护的时候。

IT/OT 必须共同协作完成制造网络安全工作，同时避免计划外停机并保护公司利润。



### 客户案例：安塞尔

虽然安塞尔以为工业领域提供个人防护用品而闻名，但公司自己网络安全也亟待加强。

IT 基础设施总监 George Michalitsianos 表示：“我们基本上是从零开始，因此，我们需要利用每个可用的安全解决方案来降低风险。通过思科安全企业许可协议 (ELA)，我们可以获得所需的所有安全解决方案，但成本只有单独购买各安全解决方案的三分之一，这无疑是前所未有的。”

由于 ELA 允许安塞尔增加多个安全产品的许可证数量，这使得安塞尔更便捷地为通过收购获得的新站点提供加入支持，并以低成本使新站点符合其全球安全标准。安塞尔还可以通过消除未集成且需要单独管理的单点产品来简化其安全实践。

通过跨多个思科安全产品 - 如思科高级恶意软件防护 (AMP)，云网络安全 (CWS) 和云邮件安全 (CES) - 集成的自动化安全功能，安塞尔每日可以拦截数以千计的高级和已知威胁，可阻止钓鱼攻击、勒索软件和已知的恶意攻击者。

一旦出现安全漏洞，思科 FireSIGHT™ 管理中心可提供集中可视性和情报，IT 员工可以通过单一管理平台对事件进行更快速的检测、遏制和补救。

[➔ 了解详情](#)

# 结论：

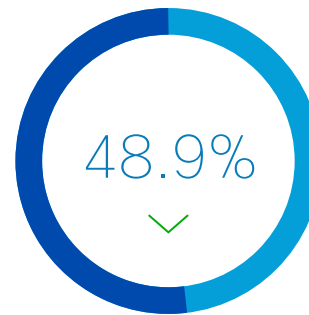
## IT/OT 融合新世界带来了前所未有的业务成果

IT和OT融合正以难以想象的方式令制造业转型，在这个过程中 IT和OT团队能更高效完成各自的工作。

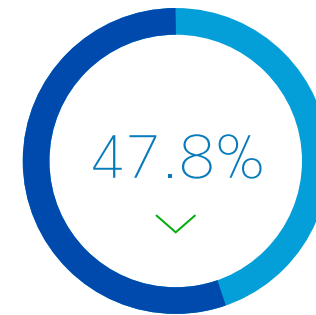
“2015 智能制造和物联网调查”显示，智能制造可促成巨大的业务成果。该调查由 SCM World 和思科共同进行，面向 418 位制造业务部门的高管和工厂经理<sup>4</sup>。

同时，凭借OT团队对生产业务的洞察，IT团队在和试图对企业实施网络攻击的黑客对抗时，也能做到“魔高一尺，道高一丈”。

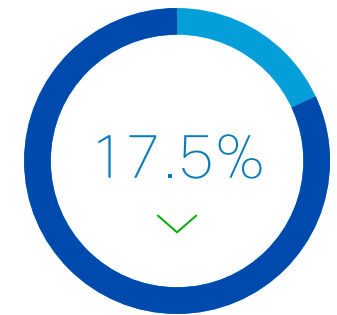
两个团队更加紧密的合作会为企业带来更多商机。虽然他们的工作方法、人员背景和业务绩效指标不尽相同，但二者都是企业实现“智造转型”中的重点投资部门。



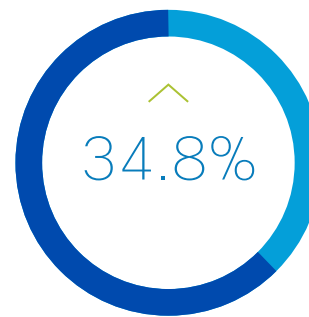
缺陷率  
下降



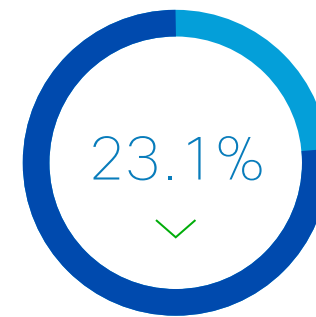
意外停机  
减少



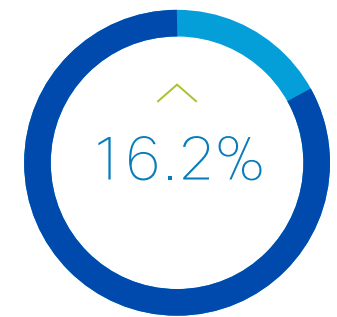
年度能源成本  
下降



库存周转率  
提高



新产品推出周期  
缩短



设备综合效率  
提高

4. <http://www.cisco.com/c/dam/assets/docs/becoming-smarter-manufacturer.pdf>



# 与我们联系

思科帮助IT和OT团队协作，来达到降低成本、提高利润、增强安全、提升效率的全数字化制造目标。您准备好迈出下一步了吗？

有关本白皮书所涵盖的各领域思科解决方案的详细信息，请访问：



01. 雾计算



02. 预测性维护



03. 工厂无线



04. 网络安全

通过思科了解有关制造业的更多信息



美洲总部  
Cisco Systems, Inc.  
加州圣何西

亚太地区总部  
Cisco Systems (USA) Pte.Ltd.  
新加坡

欧洲总部  
Cisco Systems International BV  
荷兰阿姆斯特丹

思科在全球设有 200 多个办事处。地址、电话号码和传真号码均列在思科网站 [www.cisco.com/go/offices](http://www.cisco.com/go/offices) 中。

在社交媒体上与我们联系或  
访问我们的企业网站



思科和思科徽标是思科和/或其附属公司在美国和其他国家或地区的商标或注册商标。有关思科商标的列表，请访问此 URL：[www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks)。本文提及的第三方商标均归属其各自所有者。使用“合作伙伴”一词并不暗示思科和任何其他公司存在合伙关系。(1110R)