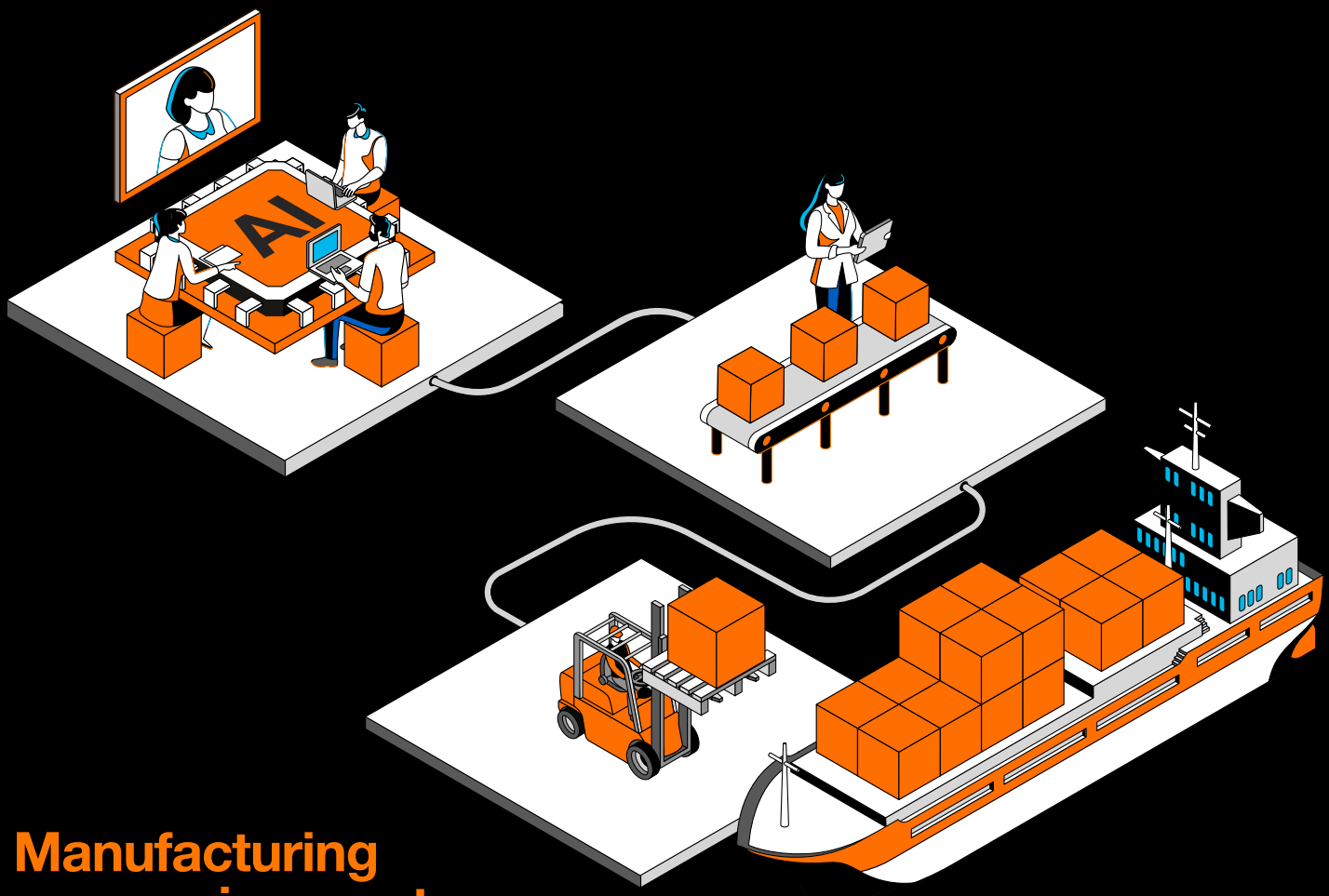
Business | Cisco Partner

The innovation/risk conundrum all industrial companies must confront – and how to resolve it

Secured by Cyberdefense



Manufacturing companies must pursue the innovations that will deliver Industry 4.0 while managing the inherent risks of doing so – but companies treating this as a purely IT problem will not realize the outcomes they seek.

The direction of innovation for all industrial companies lies in implementing the Industry 4.0 technologies that will deliver the Next Generation factory environment.

This might take several different forms - predictive maintenance, Supply Chain Optimization, greater personalization of the customer experience, Data-Driven Decision Making, more sustainable operations, or workforce transformation.

A Platform for innovation

Whatever solution you want to deliver will rely upon a strong, performant, and reliable IT layer. For example, to support the latest generation of Autonomous Guided Vehicles (AGVs) or even Unmanned Aerial Vehicles (UAVs or drones), you might wish to upgrade your wireless networks to the newest WiFi 6 or 7 specification – you might even consider implementing 5G-based Private Mobile Radio Networks.

Also, many applications commonly used to support Industry 4.0 initiatives, particularly those involving new (Gen) AI-based use cases, will be hosted in the cloud. This may require you to improve connectivity in your factory premises to provide the low-latency access that will ensure these solutions perform effectively in real-world situations. You might also find that you will need to invest further in Power over Ethernet (PoE) technology that provides power and connectivity over a single cable – many of our industrial customers are finding that this also simplifies installation and reduces costs.

The point is that many of those in charge of Industry 4.0 projects dramatically under-estimate the extent to which the factory network is now as critical as heating, ventilation and air conditioning (HVAC)). The IT Infrastructure has now become a critical asset in the production capabilities of most of our customers, with an incident on the network layer often stopping production completely. We can only conclude that, in many cases, the infrastructure is simply not up to the tasks it's currently being asked to perform – and will not support the future development of Industry 4.0 initiatives which will inevitably be implemented on the production line. This not only carries risks for your existing operations – with problems ranging from cybersecurity vulnerabilities, system downtime, data loss, and difficulty integrating new technologies – but will serve as a huge brake on future innovation.

Risks outpace the resources necessary to manage them effectively

As we've seen, the Next Generation factory requires greater connectivity. Connectivity to the rest of the organization, to customers for on-demand manufacturing, to providers for an integrated supply chain, and to the cloud for applications. All of these connections create additional risks which must be mitigated – a challenge for which the production environments of many industrial companies are ill-prepared.

Partly, this is due to the environment: there are numerous legacy systems and infrastructures in industrial locations, many of which were never designed to operate in an IT world where cyber threats are ever-present. Partly, this is to do with access to skills (a recent GlobalData survey commissioned by Orange Business found that 32% of respondents listed a 'lack of staff with appropriate skills' as a major stumbling block in implementing a digital solution in the OT environment). Also, we all know that the risks facing manufacturing companies are increasing faster than the budgets available to address them.

Treating IT as a machine

So, how can you embrace the innovation you crave while managing the inherent risks of doing so?

Well, there is no shortage of technology vendors willing to come in and try to solve these problems. However, factory leaders are rightly sensitive about handing over control of their production environments.

Also, the inability of many IT vendors to recognize and adjust to the unique requirements of Operational Technology (OT) environments causes entirely predictable problems. The GlobalData survey discussed earlier found that 38% of respondents struggled with the poor performance of an external professional services vendor, while 34% said the digital solution was not correctly configured for the actual production environment.

In many cases, the inability to distinguish between users and operators is at the root of the problem. In an IT environment, users who encounter a problem are unlikely to try and fix it themselves. However, on the factory floor, operators are required to intervene if an issue arises with plant equipment. This is one of the main reasons why many of the IT Service Management models we work with in the enterprise world are not well adapted to the OT environment.

So, your partner needs to see IT as a machine, providing training and allowing OT operators to intervene – to an appropriate degree – so they can fix problems on the IT layer. The partner will also have to have relationships with the major equipment manufacturers so that they can come in and do major repairs.

A solution aligned to your needs

Given the constraints described above, a managed service is the logical answer – but that is still no guarantee of success. The World Economic Forum found that 70% of Industry 4.0 pilots failed to move beyond the pilot phase of development - so how can you de-risk your Industry 4.0 project and improve your chances of delivering success?

The first step is to improve visibility into the OT environment, and that is where Orange Business's services come into play. The IT world, and more specifically the IT security domain, has made identifying risk a core pillar, whereas our services concentrate on visualizing IT risk in OT environments.

That's why the partnership of Cisco and Orange Business is so unique – and so perfectly aligned with the needs of industrial companies. It marries the market-leading embedded OT security expertise of Cisco's product portfolio with the service expertise of Orange Cyberdefense.

Cisco Cyber Vision provides visibility into industrial IoT and Industrial Control Systems (ICSs). This allows IT and OT teams to understand their OT security posture and work together to implement best cybersecurity practices that maintain uptime and operational efficiency. Orange Business provides the connectivity layer, and Orange Cyberdefense provides the security layer expertise, including detecting and identifying threat capabilities.

This is all wrapped in bespoke strategy, design, and integration consultancy. Orange Cyberdefense's research capabilities and proprietary database are the key reasons that its intelligence services are so sought after by multinationals around the world. For example, it is also one of the very few MSPs with an inland presence in China.

Securing the digital OT infrastructure

A European optoelectronics leader had limited visibility into OT networks and devices, which hindered its understanding of the potential attack surface and consequent vulnerabilities. It was therefore subject to targeted cyberattacks on its operational systems that resulted in lost business and increased costs from outages, and also raised the prospect of higher insurance costs and reputational damage.

Orange Business conducted a security vulnerability assessment before implementing a refreshed Industrial LAN and real-time threat monitoring with Cyber Vision software. This was integrated with the existing IT and Operational infrastructure to enhance management of security events and incidents and improve risk mitigation through increased visibility of security vulnerabilities. Overall, the solution expanded insights and drove better business decisions through Cyber Threat Intelligence and reduced reaction and response times to security events.

The combination of our strengths is how we deliver an end-to-end solution that secures the digital transformation of your production environment. And this is no marriage of convenience – Orange and Cisco have a 30-year history of collaboration that extends as far as joint development of products. The depth of our relationship may go some way to explaining the very high degree of satisfaction achieved with our customers – a recent InfoProDigital survey found that 91% of companies believe our combined solutions have significantly improved the security and productivity of their infrastructures.

Resolving the innovation/risk conundrum

This is how you can accelerate the digital transformation that will power your future while managing the risks that would compromise your current operations. No activity is entirely risk-free but, if you apply the correct methodology, your risk appetite becomes structurally better defined – allowing you to make better, weighted decisions that will help you overcome the innovation/risk conundrum.

[1] https://www.industryweek.com/technology-and-iiot/iiot/article/21267880/70-of-companies-industry-40-projects-fail-a-new-center-hopes-to-turn-that-around