What I wish I'd known

Managing the successful convergence of IT and OT

Managing the successful convergence of information and operational technology is central to protecting your business and achieving crucial competitive advantage

"The successful convergence of IT and OT is increasingly part of the board's agenda

The convergence of IT (information technology) and OT (operational technology) is not a recent phenomenon.

Industrial control systems (ICS) have been connected to IT infrastructure, providing remote connectivity for real-time data and remote support, for years.

With the fourth industrial revolution driving more intelligence, automation and optimisation, IT and OT integration is changing the way we do business. But to what extent? As the two become increasingly integrated and reliant on off-the-shelf technology, managing the convergence and the associated risk is now critical to businesses seeking to gain competitive advantage, become more efficient, profitable and reliable.

The successful convergence of IT and OT is increasingly part of the board's agenda. Securing OT or ICS is ranked as joint third in cyber leaders' digital transformation initiatives for the next 12 months, according to Deloitte's 2019 Future of Cyber Survey.[1]

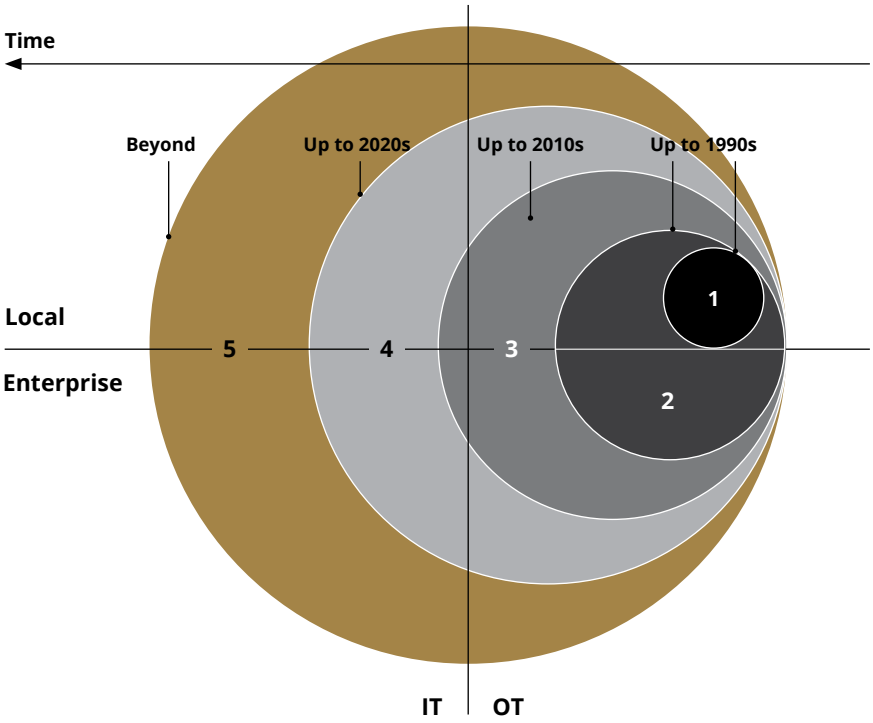
So let's dispel the myths and consider the principles behind the successful convergence of IT and OT. There are things that we know we know – the known knowns – those we know we don't know – the known unknowns – in addition to the unknown unknowns, which we don't know we don't know. As we face an ever-changing digital landscape, what questions do you, as a business executive or cyber professional, need to ask to get it right?

Known knowns

Do you know how safe your operational environment is? Securing your IT and OT integrations does not secure your plant or assets. There is a separate initiative which has its own unique set of challenges. IT/OT convergence is emerging as a hot topic in direct response to the increasing prevelance of recent industrial cyberattacks, alongside the introduction of new techniques and threat actors. A large number of these recent attacks are caused by online attackers exploiting weaknesses in more complex ecosystems and compounded by poor security of the IT/OT integration and the OT.

Essential technology to deliver the industrial product or service

1. Isolated ICS **2.** Isolated OT **3.** Reliance on IT
4. Industry 4.0 **5.** Fully converged technology



The expanded attack surface means that all sorts of industrial facilities, including oil and gas, utilities, transport and logistics, manufacturing and nuclear, are now more vulnerable to a cyberattack. Attacks levelled against industrial targets doubled over a six month period in 2019 alone.[2] Further, 90 percent of OT-sector companies have reported at least one security compromise to their infrastructure[3] in the previous two years, resulting in the loss of confidential information or disruption to operations.

According to research from Forrester and Fortinet, 56 percent of organisations using ICS not only report experiencing a breach in their OT systems during the previous year, but 97 percent say that many of these security challenges were the direct result of their IT/OT convergence efforts.[4]

It is, therefore, no surprise that 65 percent of manufacturing, mining, oil and gas, and utility companies see cyber security as their highest priority in IT and OT governance.[5]

Implementing a successful IT/OT cyber security strategy is vital.

> "Examine why you are looking at IT/OT convergence in the first place and ensure any benefits far outweigh the risk of connecting your most valuable assets

Not only is it key to ensuring the safety of your critical systems, but also to enable you to realise significant long-term benefits of convergence. These include improvements in performance and productivity, greater transparency into operational processes, and a reduction in production costs.

Known unknowns

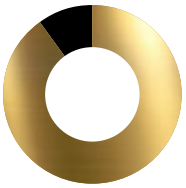
Take your own organisation; it's likely your IT and OT functions haven't overlapped and historically operated as separate organisational silos. But the interdependence of modern IT and OT systems means there is now one overarching question or unknown when it comes to securing those systems: who is accountable for operational risk?

IT/OT convergence is not a technical problem. The challenge is in overcoming culture and governance issues, which are difficult to get right. With so many stakeholders involved across the business, with different motivations, drivers, culture and competing objectives, you first need to identify everyone's role, and determine who should take accountability and who should take responsibility for securing the critical processes.

Getting stakeholders comfortable with being accountable, rather than directly responsible, will take time to work through. To achieve this you need 'purple people',[6] those who are able to build multi-disciplinary teams that have common goals and drivers, and can find a common language between the two worlds.

Also getting the different enterprise functions to collaborate is critical. For these two technology domains to come together effectively, they need to respect and address each other's concerns. For example, IT security worry they will be heavily impacted by the OT environment, which they perceive to be the "security wild west", while OT fear the IT security teams will shut down their operations, causing significant financial, reputational, and health and safety consequences. As a result, IT/OT convergence needs to be a business initiative, rather than a separate IT or OT project.

Examine why you are looking at IT/OT convergence in the first place and ensure any benefits far outweigh the risk of connecting your most valuable assets. This needs to be done holistically and on a case-by-case basis.

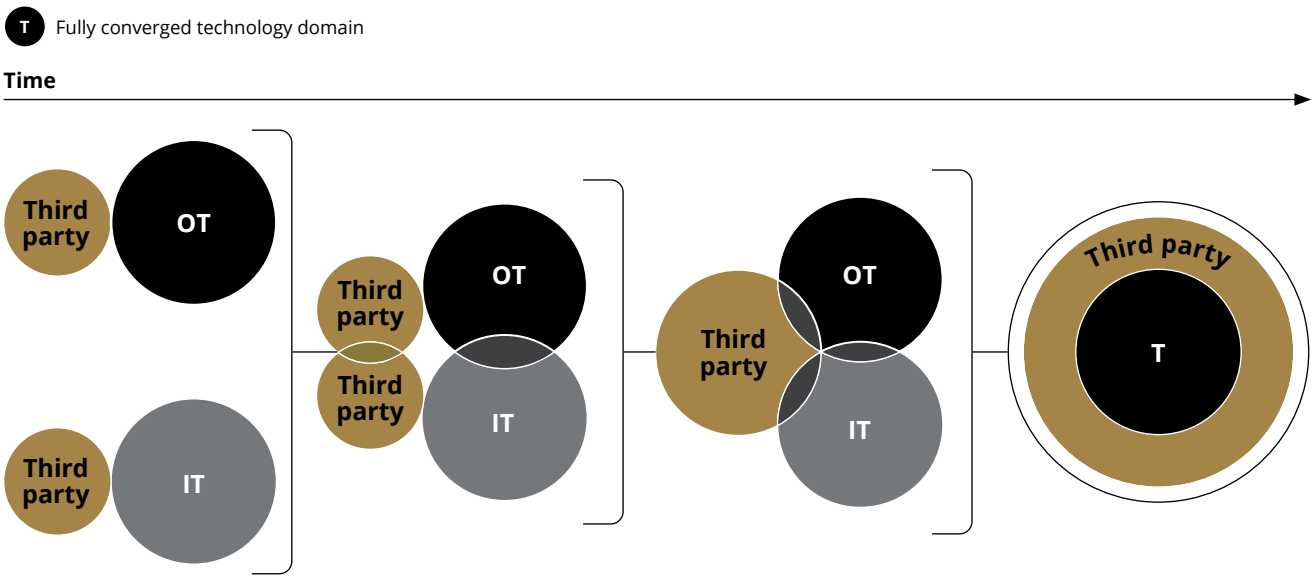


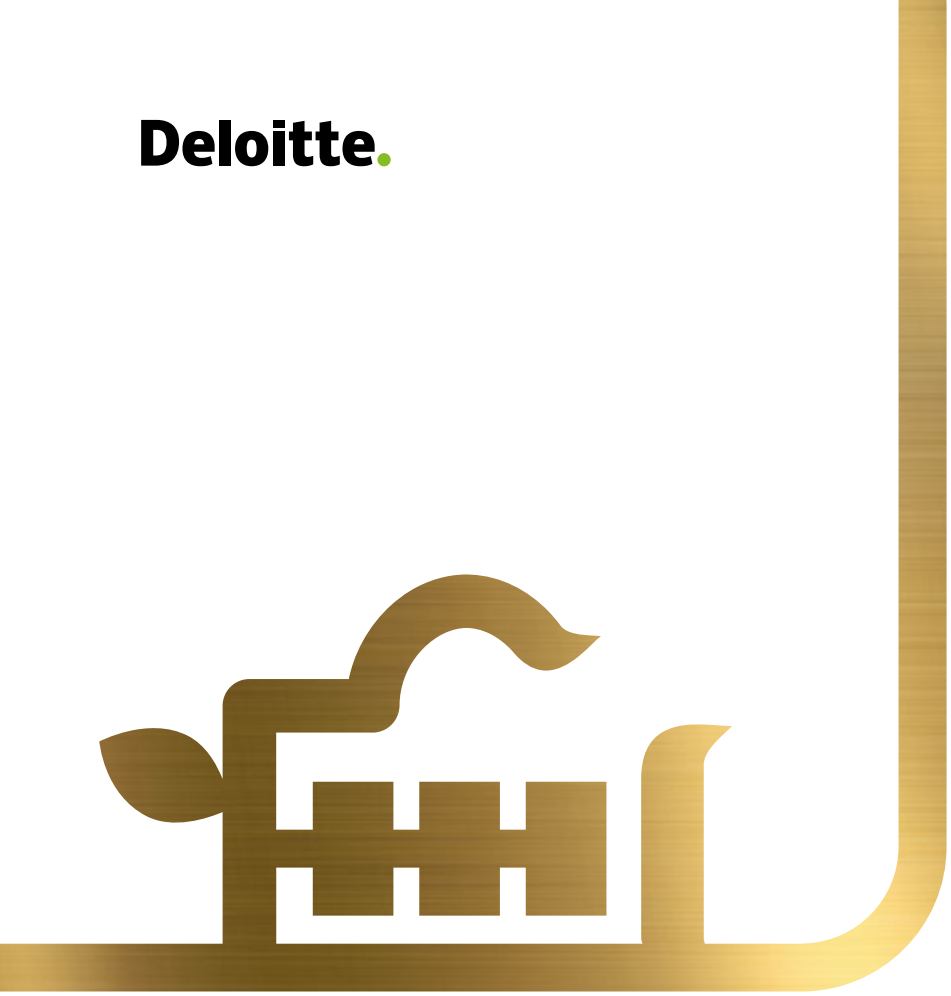
90%

of OT sector companies have reported at least one security compromise to their infrastructure in the previous two years resulting in the loss of confidential information or disruption to operations

Deloitte 2019

Converging technology environment critical to delivering industrial products and services





56%

of organisations using industrial conrol systems experienced a breach in their OT systems

Forrester and Fortinet 2019

Have a long-term vision of how you align to your business goals and what you want to achieve operationally, and only then how technology can help you achieve it. It is impossible to apply security best practices unless you have a thorough industrial-related knowledge of the operating environment and what the organisation wants to achieve. Mapping your systems to your critical business processes will enable you to prioritise your security efforts and capabilities.

And there's no such thing as too much security, right? Wrong. Security can't be too restrictive or you can add risk to the environment, rather than mitigate it, for example trying to enforce enterprise frequency password changes in safety critical environments. Securing the OT environment and the IT/OT integration is challenging. Enterprise techniques, processes and tools are not as effective, can be incredibly costly to implement and can cause issues. Not to mention the legacy systems, which cannot be updated, secured or swapped out without great cost and risk. This is why a knowledge of the operating environment and real pragmatism is required.

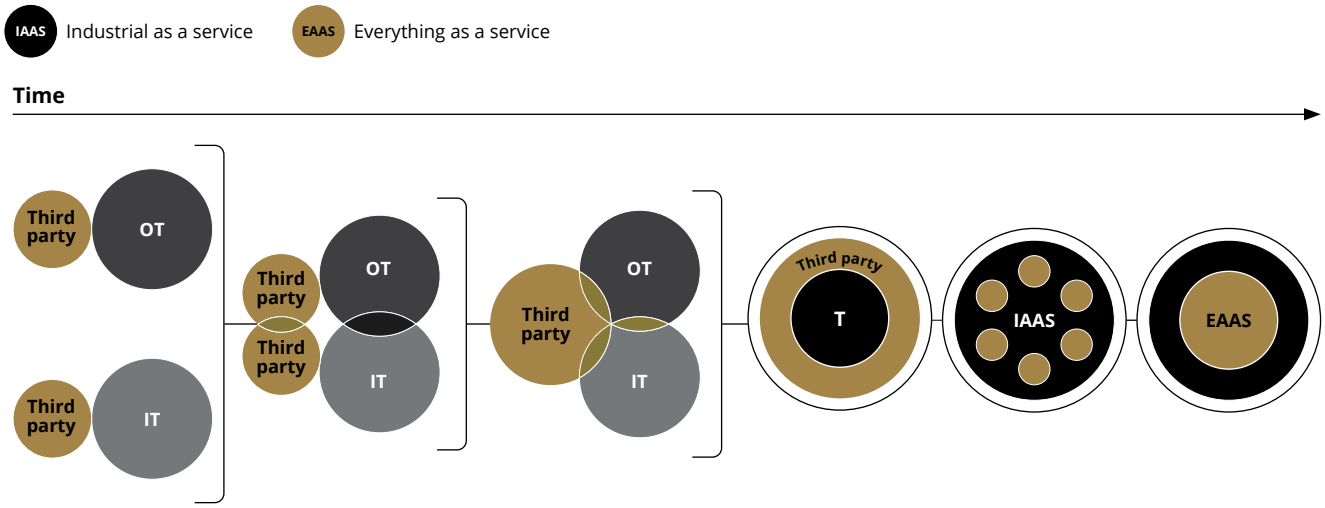
The Forrester study also reports that organisations using ICS are adding to their risks by allowing technology and other partners a high level of access into their systems. This opens businesses up to risk as the integrated supply chain is an increasingly common channel through which cyberattacks happen.

Our Third party governance and risk management 2019 survey[7] reports that supply chains and networks are becoming broader and longer. Not only are organisations subcontracting to third parties, but third parties are subcontracting to fourth parties, fourth parties to fifth parties, fifth parties to sixth parties and so on.

Only two percent of survey respondents identify and monitor all subcontractors engaged by their third parties. And a further eight percent only do so for their most critical relationships. The remaining 90 percent do not recognise the need or have appropriate knowledge, visibility or resources to monitor subcontractors. We are already seeing how this is playing out; according to the Ponemon Institute, 59 percent of companies have experienced a cyber

> "You should not consider these processes in isolation any longer; they are integral to protecting your business and achieving significant competitive advantage

Shift of control and power



incident caused by one of their vendors or third parties.[8]

Greater internal and external integration is leading to new business models, particularly in the industrial and utilities sectors, which focus on delivering a service, rather than a product. We have seen this in the transportation industry already with airlines buying "power by the hour", creating advantage in terms of reduced capital outlay, continuous monitoring and improved reliability. However, delivering an end-to-end service, including remote monitoring and configuration, means these vendors accumulate masses of data and intelligence, making them potential targets for cybercriminals.

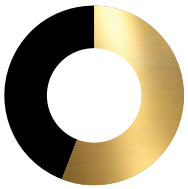
It's important to address any legal, contractual, commercial and liability issues that may arise from working in these new business models. With so many of your systems integrated internally, the probability of you invalidating a contractual agreement with the vendor, and thus being responsible, is high. Then there is the possibility that your systems could be compromised from those of other organisations connected to the same vendor.

In a world where we are drifting towards an EAAS (everything-as-a-service) model, how can you minimise or mitigate the risks?

Your unknown unknowns

Organisations are at the start of understanding the extent of their IT/OT convergence journey, what it is, why it's important and what they must do to ensure the success of a fully integrated technology domain. Do you have a vision for what a fully integrated tech domain should look like? And how will you shift the organisational mindset to foster collaboration between previously siloed departments?

The scale of change involved should not be underestimated, nor the unknown consequences of these divisions ignored.



59%

of companies have experienced a data beach caused by one of their vendors or third parties

Ponemon Institute 2018

It is vital to understand that appropriate governance and cultural transformation within your organisation is more important and integral to the success of any technical transformation.

At its heart, industrial cyber security is a cultural and governance issue. IT and OT teams must work together to enable operational continuity and maintain a digitally secure environment. Through facilitating an open dialogue to address these challenges, we focus on process, people and pragmatism, rather than on the application of expensive technology (although there are some useful OT cyber-tools) or costly and prohibitive controls.

We have created an integrated industrial cyber security capability, or IxCS, which focuses on the key business processes to keep your operations running. This includes the increasing breadth of IT, the IT/OT integration and the ICS/OT systems. You should not consider these processes in isolation any longer; they are integral to protecting your business and achieving significant competitive advantage. ■

Next steps:

01 Get buy-in from the all different stakeholders, including the C-suite, and determine the role each should play in the process.

02 Examine what you want to achieve as a business and ensure you understand both the long-term risks and benefits of digitalising your operations.

03 Start with changing the culture, and establish the governance through strategy and narrative, which will bring together the multi-disciplinary team and start creating the why, the how and the what.

04 Map the key business process and the related systems; get the focus right.

Antti Herrala
Partner
Cyber and Strategic Risk
antti.herrala@deloitte.fi

Karthi Pillay
Partner
Cyber and Strategic Risk
karthi.pillay@deloitte.fi

Endnotes

1. https://www2.deloitte.com/uk/en/pages/risk/articles/future-of-cyber-survey.html
2. https://securityintelligence.com/posts/from-state-sponsored-attackers-to-common-cybercriminals-destructive-attacks-on-the-rise/
3. https://lookbook.tenable.com/ponemonotreport/ponemon-OT-report
4. https://www.fortinet.com/content/dam/fortinet/assets/white-papers/WP-Independent-Study-Pinpoints-Significant-Scada-ICS-Cybersecurity-Risks.pdf
5. https://www.idc.com/getdoc.jsp?containerId=US44527618
6. https://www2.deloitte.com/us/en/insights/focus/cognitive-technologies/artificial-intelligence-purple-people.html
7. https://www2.deloitte.com/uk/en/pages/risk/articles/third-party-governance-risk-management.html
8. https://www.businesswire.com/news/home/20181115005665/en/Opus-Ponemon-Institute-Announce-Results-2018-Third-Party

Deloitte.