PROTECTING OPERATIONAL TECHNOLOGY

Macrium Software
It's our business to protect your data

www.macrium.com

“BEST OF BREED, BEST OF BOTH”: PROTECTING OPERATIONAL TECHNOLOGY

Operational Technology (OT) security has become increasingly critical as Information Technology (IT) and OT systems converge. That convergence makes a lot of sense: common standards and skill sets are usually a way to trim costs and extend the value of processes and the data they create, all for the good of the business. But OT isn’t IT. It lives in a world with very different priorities. At Macrium, we think there are plenty of synergies, but also plenty of points where full convergence is some way off, and smart technologists need a “best of breed, best of both” approach.

The convergence of IT and OT – a status update

There's a lot of buzz about IT/OT convergence, so let's look at the basics.

IT is the core set of technologies that power our digital domain. It's good at data storage, categorisation, and processing, and with that data we've invented whole new classes of service, supported by cloud, ever faster processing speeds and AI (to name but a few). IT connects us with our data and makes it available to applications.

OT, meanwhile, is a set of technologies that control our physical domain. In business, that typically means production lines (which are increasingly becoming automated), but it applies to us all: OT keeps our lights on and our water flowing.

And just as IT has digitised so much of our work, it is now bumping up against Operational Technologies which were traditionally mainly mechanical. They were digitised systems which controlled machines. Redhat say that OT "includes industrial control systems (ICSs) like programmable logic controllers (PLCs), distributed control systems (DCSs), and supervisory control and data acquisition (SCADA) systems"; alongside a fairly bespoke collection of industrial-focused PCs. This traditional OT sometimes produced a lot of data, but didn't use it for much that was useful, particularly as it usually operated unconnected, often on discrete and custom-manufactured pieces of digital tech.

All that has changed with the Internet of Things (IoT), a connected and generally lower-cost digitisation of mechanical systems which means that machines increasingly have a connected digital layer on top. For example, sensors can tell when a machine is about to fail or a component is reaching the end of its useful life; and notify someone. That means maintenance can be scheduled according to need (rather than guesswork) which in turn cuts factory costs. And because problems can be predicted rather than tackled as an emergency, supply chains are less affected by shutdowns, increasing efficiency and cutting costs even further.

Connected OT is therefore very popular, but IT and OT are not natural bedfellows. It's not a convergence, it's a collision. In the past, those ICSs and industrial PCs lived in splendid isolation. Most control systems for industrial units haven't been networked at all:

Control was originally manual, and specific to the device. Different manufacturers created their own bespoke methodologies and operating systems. Experts using machines were more indispensable by being specialists on that machine too, so interoperability was in nobody's interest.

And unlike office computer equipment which has experienced constant downward price pressure, industrial equipment is capital intensive. Once a company had bought into a manufacturer, they were in for the long haul. The IT estate for most businesses is now a healthy blend of interoperable OEM computers, clouds and devices with a buying cycle of just two to three years. The buying cycle for industrial equipment, conversely, is often locked-in, multi-million pound investments, depreciated over 10-20 years.

Worse still, where that industrial equipment was computerised, it usually wasn't with a typical PC. The software, operating system and device would have been in the hands of the equipment vendor. That device was often onboard and non-serviceable. And because hardware is often designed to have a long life, updating the software was not seen as necessary for discreet machines and devices, as it was often written for a limited purpose.

Thus, the digitisation of OT has been slow. There have been interoperability standards (most notably SCADA), but it's taken the arrival of IoT and Industry 4.0 (which IBM nicely describes as "the realization of the digital transformation of the field" for manufacturers and heavy industry to want to digitise).

A different risk profile

But the challenge isn't just that OT has taken time to catch up. The discipline of OT has an entirely different risk profile to IT. The reason OT has remained resolutely unnetworked is that cybersecurity risks in the manufacturing world stack up fast:

The cost of disruption to a production line can cost thousands of times more than the disruption to a data environment. Unlike some service sectors, where downtime might mean nothing more than some missed emails or a few days working from home, in manufacturing the effects are immediate and painful.

According to IioT World, "unplanned downtime in manufacturing can cost a company as much as $260,000 an hour" – indeed firms they surveyed reported typical "outages lasted an average of four hours and cost an average of $2 million". Other sectors are even more challenged: the long supply chains and just-in-time processes of automotive manufacturing means that downtime on a car production line is around $50,000 per minute; and downtime in the energy sector often breaks through $2.5m per hour. Evocon, meanwhile, report that "Unplanned downtime now costs Fortune Global 500 companies 11% of their yearly turnover, almost $1.5 trillion. The annual cost of downtime is now $129 million per facility among Fortune Global 500 companies."

Despite the fact that IT security challenges can cost millions in reputational damage - and we would never denigrate its importance - an OT cyber attack can mean damage to critical national infrastructure – and that means the knock-on effects are far more than reputational; and can affect whole communities.

And finally, OT disruption can't always be clawed back. If a digital IT system is down for even whole days, transactions can catch up, deals can still be done, the office can stay open. If however, for example, the technology behind a solar farm is compromised, that energy – and its value - is lost forever. In automotive, meanwhile, whole supply chains can snarl up, and value is permanently lost.

Now apply those risks to the sort of OT estate we discussed above. A multi-generational estate with systems of varying ages on different upgrade cycles from different manufacturers. Old systems which may even lack vendor support and operate on a legacy OS. Plenty of industrial systems are currently native to Windows XP, for example, which is a tremendous operating system but long out of support. That sort of estate is difficult to update or patch, increasing its vulnerability to cyber threats.

We simply cannot apply the same universal standards to OT as have become the norm for IT. No wonder the sunlit uplands of a universally connected, networked and perimeter-protected integrated IT/OT operation feel ambitious at best.

Now add new pressures...

While the risks are high, there are also new pressures and incentives to live up to. First, as we find ourselves in a more challenging and combative geopolitical environment, OT has become an attractive target for bad actors, some of whom are state-sponsored. You may remember Stuxnet. CSO Magazine called it "the first known cyberweapon", and it was designed by US and Israeli specialists specifically to target OT in Iran's nuclear weapons programme. Since then, OT has been the focus of many attacks, precisely because a relatively small investment in malicious time and effort can yield dramatic costs (see above) and therefore an incentive to e.g. pay a ransom, fast.

Second, the cost of cyber insurance is rising, precisely because of the cost profile of OT attacks; and also because insurers don't necessarily understand OT and have been bundling it with IT risk. The Cyber Insurance Academy recently called OT "the Wild West", writing, "Many CISOs experience some push back from engineering teams when it comes to managing cyber risk for OT, with many struggling to see OT as a significant exposure. OT often runs on outdated Operating Systems which are often impossible to program to today's cyber hygiene minimum benchmarks. Therefore, many CISOs lack the resources to effectively address OT exposures, which can create critical gaps in an entity's cyber security and business continuity programs... Insurers who fail to conduct effective underwriting and collaborate with their clients may be unexpectedly exposed to operational technology (OT) cyber risks." Once burned, insurers are hiking prices.

And third, American and European companies (and the UK is following their lead here) are obliged to meet stringent new cybersecurity standards defined under the NIST Cybersecurity Framework (US) or NIS 2 Directive (EU). Energy, transport, healthcare, manufacturing and water services are all identified as critical sectors in NIS 2, with penalties of up to €10m or 2% of a firm's total global annual turnover for non-compliance. Industrial Cyber reports, "The path to compliance involves adopting a risk-based approach to risk management, where organizations leverage existing information and insights to prioritize risk mitigation efforts." But despite being well-intentioned, the legislation is also leading to something of a skills shortage.

OT manufacturers for the energy sector, Landis+Gyr, note "NIS 2 will suddenly increase the number of companies within the EU that are legally obliged to ensure cyber security to over 400,000." NIS 2 brings new obligations, and fewer people to fill key roles. It is essential that you automate whatever you can. For example, as well as being compliant, a core obligation of NIS 2 is being able to demonstrate that compliance. Your security systems must include reporting to show that your risk-based approach is being observed at all times. Macrium backups include fully-featured reporting, easy data extraction and human-readable log files for forensic auditing, should you need to dig into the records after an attack or report back for compliance purposes.

To find out more about how Macrium can help protect your manufacturing operations, speak to one of our experts.

SPEAK TO AN EXPERT

Protecting data and processes from multiple IT and OT sources

So what can you do to protect IT and OT systems in a coherent way? Well, the processes might be slightly different, but the objectives and themes between IT and OT are very similar:

Establish your KPIs

What does good look like? Both IT and OT cyber protections have clear objectives for recovery planning, even though the requirements for OT will almost certainly be more demanding.

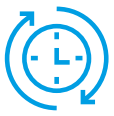
Typical KPIs are:

Recovery Time Objective (RTO)

The maximum acceptable amount of time to restore a system or process after a disaster to avoid unacceptable consequences. As we saw above, the RTO for OT is usually measured in minutes rather than hours or days. Furthermore, the RTO in an OT context should be assessed at a device level. Unlike IT systems which can usually be managed at a departmental level or higher, individual OT devices can be the difference between keeping the lights on and a trickle down series of expensive failures.

Recovery Point Objective (RPO)

RPO indicates the point in time to which data must be recovered following a disruption. This will determine the frequency of your backups. OT cybersecurity specialists, Applied Risk, note: "An operation where manufacturing follows an unchanging set of protocols may require a less frequent backup than an industry that relies on a real-time data loop to inform operations." In the OT world, the RPO requirement may be very different to that in the IT world, and there may be multiple parameters. Let's for example, take a quality control camera on a production line. Rather than protecting all of the data, you may protect just what you need to recover. The camera doesn't have 2 million customer records like an office system; after a few days for compliance the pictures of each item on the production line are worthless. But the camera's OS-image is crucial and should be kept for at least six months, with multiple checkpoints, in order to protect against expensive ransomware attacks. And to ensure the device can be back online in minutes, you'll want daily or even hourly backups. In the office, it's the data you want to protect. On the production line, it's the process which needs to be restored.



Mean Time to Recover (MTTR)

The average time taken to restore a system to service. MTTR includes the time taken to diagnose the issue, repair it, and return the system to normal operation.

Data Restore Success Rate

The percentage of successful system/data restores from backup compared to the total number of restore attempts. This KPI ensures that the restored system/data is accurate and usable. Because OT systems are typically discrete and bespoke, this is a vital measure of your response effectiveness.

You may also measure system downtime, costs of downtime etc.; and there are bound to be metrics specific to your business. Equally, there will be metrics designed to face upwards, to the wider business. For example, one automotive company's number one metric is "the number of cars lost in each production/year" – because these are the sorts of numbers which affect strategy and share price.

Always Encrypt

Encrypting data at rest and in transit is essential to protect sensitive information from unauthorized access.

Implement Access Controls and User Authentication

Implementing robust access controls and multi-factor authentication (MFA) helps ensure that only authorised employees can access critical OT systems and data. This reduces the risk of insider threats and unauthorized access.

Enforce Network Segmentation

Segmenting networks helps contain potential breaches and limits the spread of malware. By isolating OT systems from IT networks, you can minimise the attack surface and enhance your overall security for both OT and IT components. It will also make forensic digital analysis easier should the worst happen, improving your MTTR.

Implement first-class Backup Strategies

Regular backups are a staple for disaster recovery, but they are crucial for OT environments. Implementing air-gapped backups, which are physically isolated from the network, can protect data from ransomware and other cyber threats.

Mind the gap...

Air-gapping might feel like an overly traditional and manual way to protect your backups. After all, someone is going to have to physically go on site to reinstall your critical data. Is it really necessary? Well, perhaps we should ask: is it $260,000 an hour necessary?

Smart Industry reports, "As ransomware attacks become more sophisticated, manufacturers and critical infrastructure operators must implement robust, air-gapped backup strategies. Air-gapped backups are physically and logically isolated from the industrial control network to prevent ransomware malware from compromising the backup systems."

Air-gapping again minimises the attack surface and ensures that your backups remain secure even if the rest of the network is compromised. That's not just good for security, it's operationally powerful because it significantly reduces your MTTR as well as your risk. You can get critical equipment back up and running even if the rest of the IT side of your network is still compromised.

Then we should also consider devices running an out-of-support OS. We talked about multi-generational OT earlier. For systems running on outdated operating systems that no longer receive vendor support, air-gapping may be the only viable security measure. This isolation prevents external access and is the only way to reliably mitigate the risk of exploitation.

Finally, we should note that while the cloud is essential for consumer-facing businesses, it still makes sense for many industrial and back-office systems to operate on-premise services, especially for backups. That's not so much an issue of expense – the transit fees to get industrial equipment back up and running won't be inordinate. It's more a case of speed. If finding and downloading the right backup (possibly of many!) from a cloud service takes a matter of hours, the cost of your incident response could be huge. Plus, cloud access relies on a safe, secure and uncompromised network. If the attack you face makes your network unusable (and that's highly likely) then the cloud is the last place you should seek rescue! This is also where OT teams are most out of sync with IT teams. For the past decade, CTOs have (rightly) driven rapid adoption of the cloud, with its compelling delivery of optimised IT running costs. There will be a time (thanks to continued improvements in connectivity, security and IIoT devices/standards) when the cloud will be a viable option for OT too, but for now it is often not, and on-premise is often the best - or even a non-negotiable - option.

Consider public keys for micro-perimeters

Some facilities will have hundreds of independent IoT (or IIoT) sensors, and in that instance you can't treat each individual sensor as its own physical location. But many facilities will have a few large units (often with multiple internal digital systems). Since we've been talking about the problems of securing these diverse units, it may make sense to use public key encryption systems – which have been tried and tested for decades – as a first line of defence. Public keys are a framework to ensure unique digitally certified identities for every user, device or application seeking network access to your operational devices and authenticating them with every request they make – effectively a micro-perimeter for each device.

Deploy Intrusion Detection Systems

Deploying these systems helps detect unauthorized access and malicious activities. These systems can identify anomalies and alert your security teams to potential threats in real-time. They should be a standard part of your cybersecurity approach.

Drill your Incident Response Plan

Having a well-defined incident response plan ensures that you can quickly respond to security incidents. But in the time-critical OT world, and with air-gapped equipment, this is a physical process which requires everyone to turn up and bring their A-game; not bringing your team together over cups of tea at home by their laptops. Run realistic drills; and if you're lucky enough not to have 24/7 operations, do your simulation off-shift for as realistic a process as possible.

By the way, by now it should be clear that while we feel OT and IT are very different disciplines, the results are far better when IT and OT teams work together. So produce a shared incident response plan, and run drills as a shared team. Share your skills and understanding of requirements. Work across the two disciplines to explain what is needed (for example your expectations on RPO and RTO per device or category) so that everyone is working towards the same goals.

It's worth re-emphasising: these steps are valid in a generalised way both for IT and OT systems; however, the outcomes you need and the resources it makes sense to put against your RTO/RPO, will likely be starkly different.

Blank sheet strategies

That's why we talk about "Best of breed, best of both": the fact that OT is starting to operate in a connected way like IT - and suffering the security challenges of that connectivity – is where much of the similarity ends.

But if you are lucky enough to be starting from a blank sheet of paper – or at least able to give IT and OT unified, strategic consideration, there are a few fundamentals to prioritise. As Tech UK, the UK's technology trade association, writes, "Do not assume all assets will be new, and do not underestimate the challenges involved in bringing together what are likely to be two very different approaches to cyber security!" You may not be able to invest immediately in these directions, but they are good "North Stars" to aim for:

Take a holistic view

OT has a raft of industrial networking standards (e.g. Modbus, Profinet and ODVA's CIP – the Common Industrial Protocol) alongside traditional IP and unconnected units, in an ecosystem of PLCs (logic controllers), SCADAs (control systems), HMIs (standalone interfaces) and industrial PCs of multiple flavours. You can't expect devices and protocols to align perfectly on security issues, and it's up to the OT specialist to take a birds'-eye holistic view of the estate.

Your talent pool

Skills are in high demand in IT – especially in cybersecurity. But that's nothing compared to the skills shortage in OT. For example, over 29,000 companies from airlines to retail, including 90% of the Fortune 500, still have demand for COBOL. One live COBOL system is 60 years old. OT is littered with bespoke (sometimes cobbled together) systems which need non-standard training to understand. To achieve a converged environment, you will need IT and OT expertise in the same room.

Macrium backups as part of your OT strategy: a top five

Backups are only one component of a holistic OT security strategy; but now that we have a fuller picture, we can see why Macrium is a sound choice:

1

Macrium supports air-gapping at any scale. You can activate licenses via your Macrium Account, allowing for installation of offline computers, and run critical backup processes in a fully air-gapped environment – whether one key computer or an entire production line (many other services only provide offline support above 100 or more devices).

2

It creates full drive images, which support Windows versions right back to Windows XP): ideal for scenarios where you're running multi-generational equipment of different ages and different upgrade cycles. Each image will back up the OS, systems, drivers, apps and custom configurations, not just data. In an OT context that often includes drivers and OS customisations which are no longer even available. Indeed, our driver harvesting and ReDeploy capabilities are credited with helping manufacturers legitimately extend the life of hardware, reducing capital costs.

3

Macrium supports "rapid delta restores". The delta is the difference between two states, so a delta restore reliably restores only the data that has changed between two restore points. This means that, for example, if a Windows machine has crashed (rather than a complete hard drive failure), only data that has changed since the last checkpoint need be restored; meaning you can get up and running faster. As we've seen, in an OT context, that can save thousands of pounds in lost productivity.

4

And Macrium can be scheduled to run backups at appropriate times, again optimising your operational value. Every company has different time windows for backups, but it's much harder to schedule backup times when you have equipment running 24/7 for 5 or 6 days a week and any backup operation must not affect hardware operation or the network. Scheduling helps with this challenge – as does reducing the backup read/write requirement by using rapid deltas as discussed above.

5

Finally, Macrium is designed to be simple to use. Resources are always challenging; OT resources are scarce, and after a cyberattack at 2am on a rainy Friday, they are even harder to find. Macrium restore processes are designed to be executed on the factory floor without specialist assistance.

6

No "top five" would be complete without a bonus #6; so let's look at an additional key reassurance. We saw above that one key – and unfortunately increasing - cause of disruption to data is malicious actors, particularly using ransomware. It would truly be a worst-case scenario to fall back on your backup, only to find that this too had been corrupted by bad actors. Macrium Image Guardian helps protect your backups from being modified by malicious users, so that a drama has a much smaller chance of descending into a crisis.

Steady progress on the path to convergence

The convergence of IT and OT promises significant opportunities for reduced cost and complexity. And it will ultimately be achieved, but like everything else in tech, it will take longer than expected, and there are many challenges to resolve along the way. While shared standards and skillsets can drive efficiency, OT's unique risk profile and operational priorities require specialised security and recovery measures. We've looked at robust access controls, network segmentation, air-gapped backups, and defined recovery objectives – all of these are essential. On the people side, collaboration across IT and OT teams will improve your resilience, keep the lights on and make convergence a smoother process in the months and years to come. Embracing a "best of breed, best of both" approach will allow your business to leverage the evolution of OT digitisation without forcing an OT square peg into an IT round hole.

To find out more about how Macrium can help protect your manufacturing operations, speak to one of our experts.

SPEAK TO AN EXPERT