The Industrial Cyber Security Principle Method™

A White Paper

SiS Next-Level Industrial Cyber Security

Contents

A message from our founder

Operational Technology and Industrial Control System (OT/ICS) security sits in a class of its own. It's often conflated with IT cyber security, which is where the problems with its proper execution lie. Because OT cyber security needs to be given the specialist treatment it deserves.

Following my completion of a cyber-terrorism and control system security doctorate over 15 years ago, I founded the company SIS Industrial Cyber Security to address a gap in dedicated OT security. There were little to very few operational technology specialists in the market locally and internationally, and my experience made it very clear to me this gap needed filling.

Just as we've seen an escalation in IT security incidents recently, OT is a vulnerable target for increasingly active and sophisticated cyber-adversaries. This is a fact that can't be ignored.

Being an early innovator in this space has given me and the SIS team a privileged perspective of what's happening across the globe and where it's heading. We've been well-positioned to come up with best-practice approaches for industry to implement and measure the effectiveness of industrial cyber security.

After working extensively with industry, testing our knowledge and our mettle, and responding to developments in the cyber security landscape, we landed on a methodology that has proven successful: The Industrial Cyber Security Principle Method™.

In this white paper, you'll get a better idea of the principles and motivations behind The Industrial Cyber Security Principle Method™. You'll see how it all comes together to create a more fortified defence for the distinct cyber security requirements affecting OT. You can also benchmark yourself against the criteria of The Industrial Cyber Security Principle Method™ and determine whether there are dents in your armour.

This is where your journey to world-class industrial cyber security begins.

Dr Christopher Beggs
Founder & Principal OT Security Consultant
PhD Cyber-terrorism & Control System Security,
Certified Industrial Cyber Security Specialist (CICSS),
Certified SABSA & SCADA Security Architect

Common Industry Problems

The Industrial Cyber Security Principle Method™ was created to address recurring problems in OT security across different industries worldwide, and to help owners and/or operators of critical infrastructure to elevate their OT security posture to a world class level.

Problem #1

Jumping to a technology solution before anything else

Too many organisations resort to technology-first approaches without properly assessing the unique business and operational security needs of their OT environments.

The Principle Method evaluates the specifics of the organisation before anything else, so technology can be deployed cost-effectively and to its greatest advantage.

Problem #2

Taking a blanket approach to OT security controls

Applying a blanket approach is unmanageable due to the complexity and array of different OT systems.

The Principle Method examines each unique system in an organisation in detail, creates a risk profile for that system and then appropriately adjusts the security controls required for each system.

Problem #3

Lack of communication across IT and OT

IT and OT are often seen as the same, which may make IT responsible for OT cyber security when they don't fully understand what's needed to do so effectively.

The Principle Method brings IT and OT together, so any communication barriers can be overcome and lapses in OT cyber security don't get lost in translation.

Problem #4

Lack of strong business case for OT security

Many people face difficulties advocating for adequate OT security investment because they're not armed with the right arguments or evidence to support their case.

The Principle Method provides a clear path for an organisation's OT security posture, which helps justify investment and outline the risk involved if proper attention is not paid.

Problem #5

Quantifying the true risk of your OT security

While organisations understand there is risk, they're unlikely to have the tools, abilities and know-how to fully quantify their risk landscape.

The Principle Method offers a thorough means for risk quantification, so organisations can grasp the realities of their OT cyber security and adopt proven tactics to fortify their risk position.

Problem #6

Underestimating the required effort to manage OT cyber threats

Effective OT security is not a set-and-forget exercise, requiring consistent management and re-evaluation to keep ahead of increasingly sophisticated threats.

The Principle Method™ acts as a blueprint for best-practice OT security across the lifecycle of an organisation's OT systems, meeting the challenges involved in sustaining long-term cyber security strength.

So what is the Industrial Cyber Security Principal Method™? ⟶

What is The Industrial Cyber Security Principle Method™?

The Industrial Cyber Security Principle Method™ is an OT security methodology created by SIS Industrial Cyber Security in direct response to the burning global need for OT-specific cyber security. It is a melding and distillation of established industry frameworks[1,2,3] with real-world experience, refined to better meet the changing nature of OT security threats.

At its core are six foundational principles:

1. Business-Driven
2. Risk-Based
3. Enterprise-Wide
4. Methodical
5. OT Security-Focused
6. OT Security-Compliant

When combined, these six principles are the vital ingredients in the SIS recipe for delivering world-class industrial cyber security solutions.

Think of these principles as the framework of a house. If you start building a house without its frame, there's no structure to control the final outcome.

Like a house framework, The Industrial Cyber Security Principle Method™ gives shape, form and integrity to your industrial cyber security protocols. It grounds your OT in away that covers all bases and ensures you have the right stuff to do three things:

- Understand your OT security position.
- Improve your OT security position.
- Respond to threats powerfully and with confidence.

Each principle builds on the other to provide a comprehensive, strategic and effective OT security posture that not only attends to immediate threats but also strengthens your operations against future cyber events.

In the SIS universe, we consider the principles of The Industrial Cyber Security Principle Method™ as the supports that anchor and inform everything we do. Our greater roadmap to world-class industrial cyber security includes assessment, technical design, management & governance, implementation, training and ongoing management.

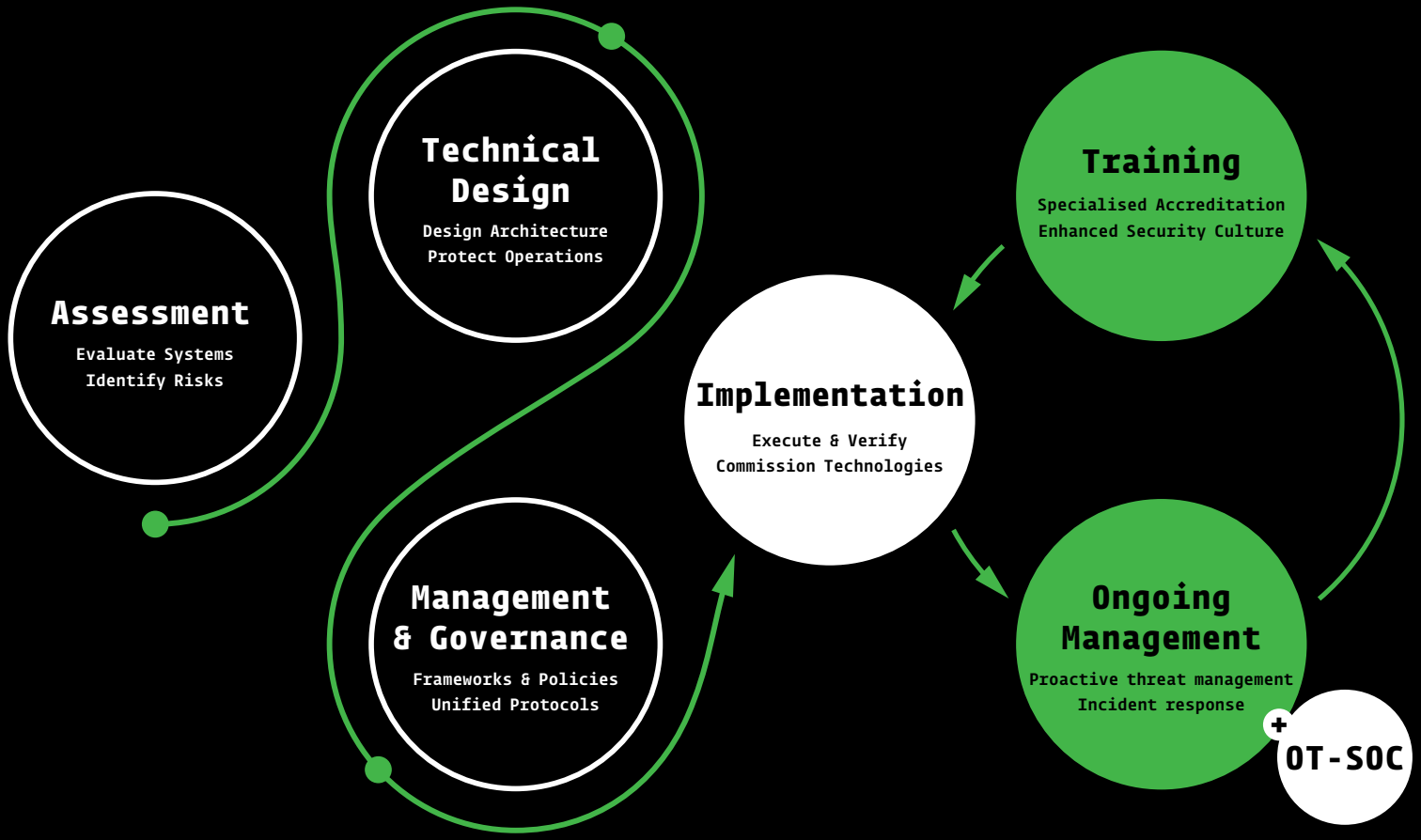
But you'll see The Industrial Cyber Security Principle Method™ underscores it all when you turn the page.

1. Theodore J. Williams (1994) "The Purdue enterprise reference architecture." Computers in industry Vol 24 (2). p. 141-158.

2. John Sherwood, Andrew Clark & David Lynas (2009) Enterprise Security Architecture Available at: https://sabsa.org/ [August 2024]

3. Michael J. Assante and Robert M. Lee (2015) The Industrial Control System Cyber Kill Chain Available at: https://sansorg.egnyte.com/dl/HHa9fCekmc [August,2024]

World-Class Industrial Cyber Security Roadmap



Problems

- ✗ Technoloy First
- ✗ Blanket Approach
- ✗ Communication Gaps
- ✗ Weak Business Case
- ✗ Poor Risk Understanding
- ✗ Lifecycle Underestimation

Outcomes

- ✓ Protect Business Operations
- ✓ Reduce Risk
- ✓ Regulatory Compliance

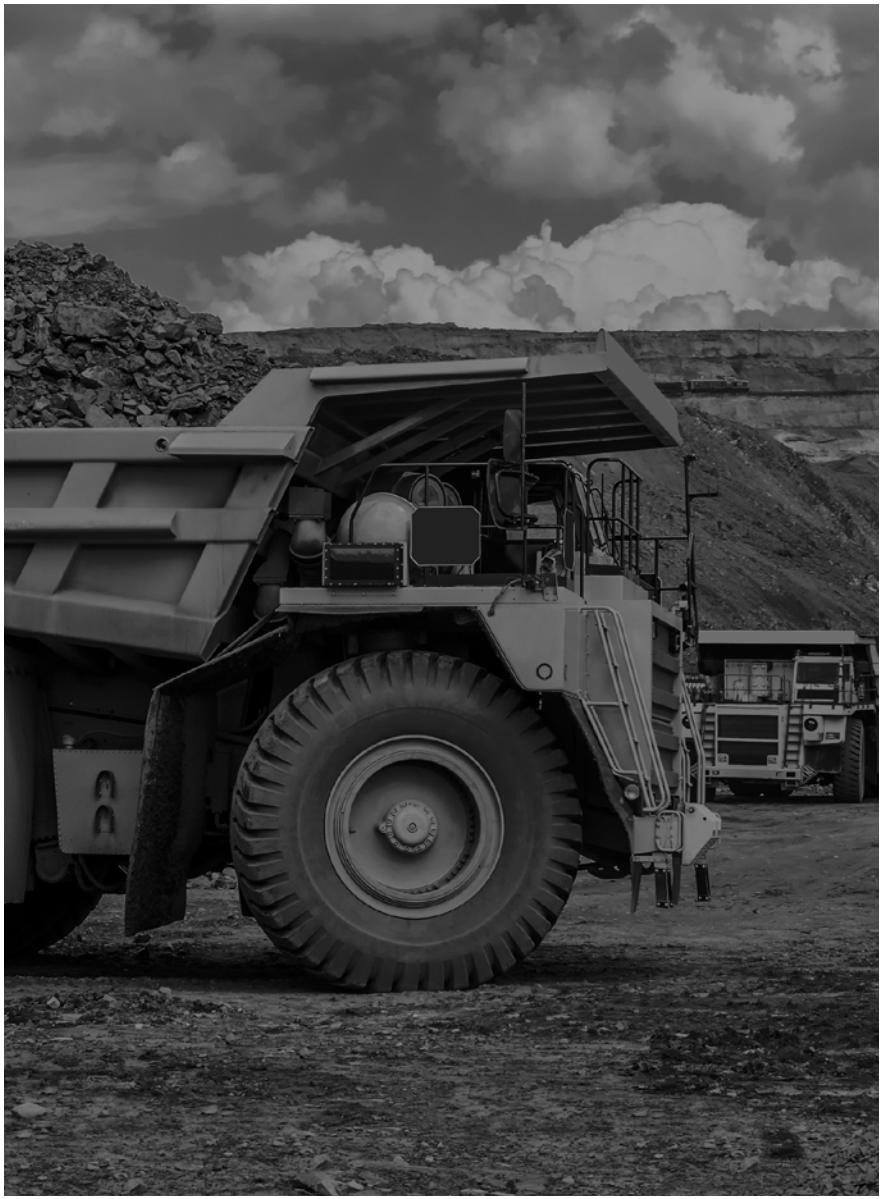
Principles

Business Driven | Risk Based | Enterprise Wide | Methodical | OT Security Focused | OT Security Compliance

1. Business-Driven

The Business-Driven Principle is about aligning your primary business functions with your industrial cyber security. It's about ensuring what you do every day – your reason for being here – is properly serviced by your OT security requirements.

Typically, the Business-Driven Principle is the first to be executed in The Industrial Cyber Security Principle Method™ because it relies on a deep process of cross-organisation discovery that can be used to inform all other principles. This involves analysing business processes for OT systems, drawing from source data and information gathered from direct interviews with operational OT asset and engineering business managers.



Nothing is assumed because no organisation is the same.

Any attempts to skip steps or take shortcuts at this important stage threaten the viability of the entire OT cyber security process. And yet, it is still common for organisations implementing OT security to fail to give this stage their full attention.

Look beyond the technical aspects of your industrial cyber security.

It makes sense for your organisation's OT cyber security team to consider the broader spectrum of operational requirements, so they can then offer genuine business support and enablement. Being business-driven also ensures any OT cyber security efforts deliver on what your organisation truly expects, wants and needs.

Key actions for; The Business-Driven Principle

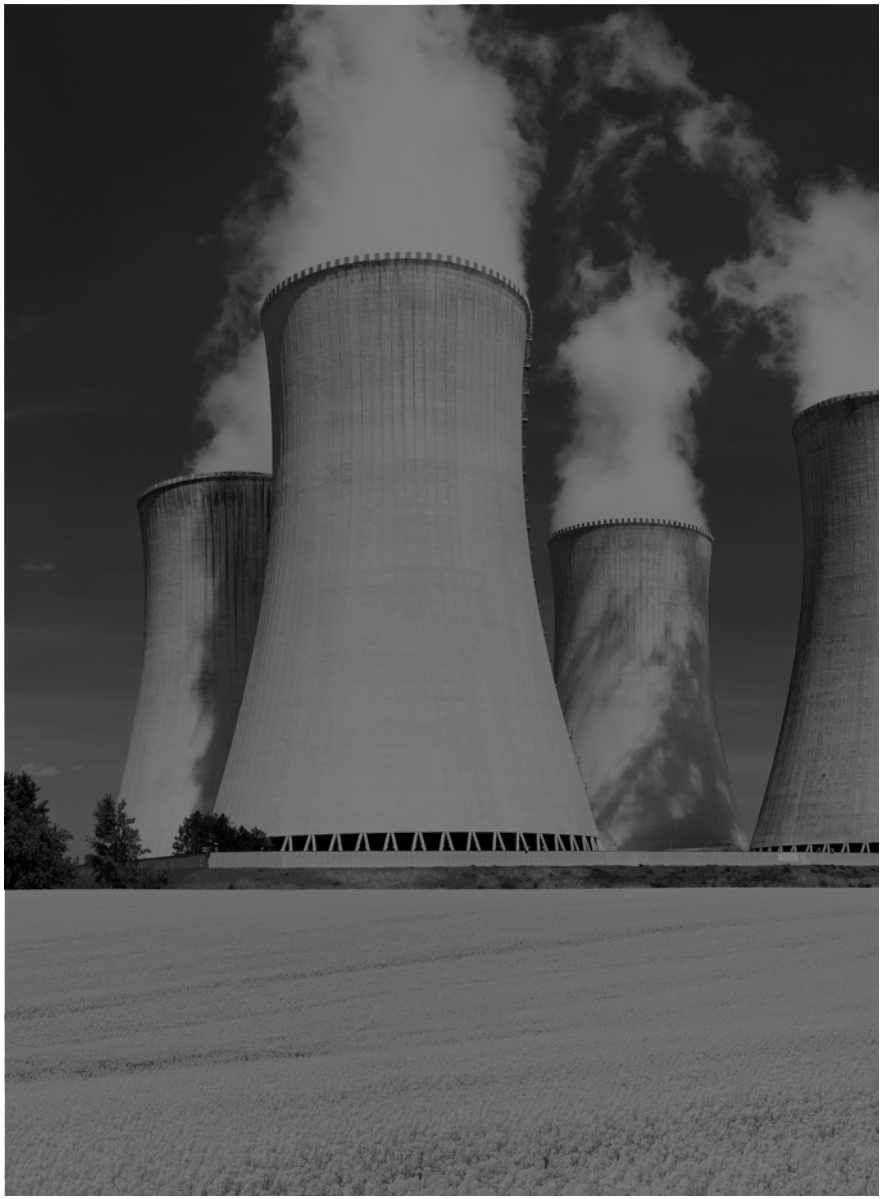
- Identifying and quantifying the business goals and strategic objectives that need safeguarding.
- Scoping and adopting a comprehensive, multi-dimensional business perspective that ensures end-to-end value delivery.
- Articulating business risks in terms of new opportunities and potential threats.
- Cataloguing integral OT business processes that require security measures.
- Analysing the organisational structure and how it interrelates with business strategies, products, policies, initiatives and stakeholders.
- Outlining the principal geographic locations of the business and their specific relevance.
- Defining critical time-dependencies and sequential aspects of OT business processes, focusing on both performance and order.

2. Risk-Based

The Risk-Based Principle is about customising your OT security to the specific risks associated with each system or subsystem in your business, rather than applying the same security control coverage across everything.

While organisations may implement point solutions for OT that provide some level of security, this is likely ad hoc. Often, no one in an organisation can confidently say whether the security level is appropriate to the risk, whether the benefit justifies the cost, or whether it meets a broader range of business requirements that aren't directly related to OT (i.e. informed by The Business-Driven Principle).

There's a reason for this...



Thorough risk assessments are challenging to execute effectively.

Many organisations struggle due to limited quantitative data, a scarcity of specialists skilled in accurately simulating cyber-attacks and cyber adversaries constantly working to evade detection. That's why it's pragmatic to engage a third-party OT security specialist to reveal the threats, both external and internal, as well as exploitable weaknesses across your business to come up with your organisation's risk profile.

The ICS Cyber Kill Chain is a best-practice model for risk assessments.

The ICS Cyber Kill Chain[3] involves simulating real-world attacks and frameworks, and then relating the findings back to your organisation's infrastructure. This process helps assess the likelihood and consequences of any threats materialising.

In addition, there's also the need and evaluation of potential simpler attacks by insider threats, such as Denial of Service (DoS) or the exploitation of unpatched vulnerabilities through techniques like privilege escalation.

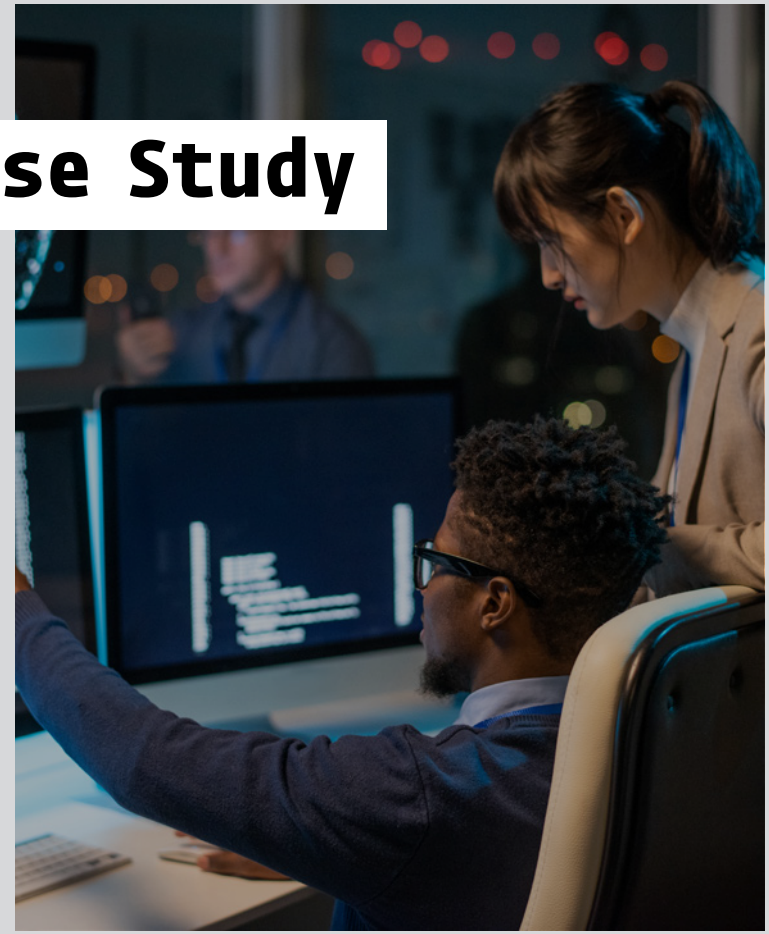
A valuable strategy is the profiling of external threats.

It is well-known that cybercrime collectives target critical infrastructure. By keeping tabs on these groups, a profile of your business can be created to see if you could be a target of specific collectives or even certain countries.

Key actions for; The Risk-Based Principle

- Adopting an ongoing risk-based mindset for all industrial security decisions.
- Undertaking a comprehensive asset class discovery across Levels 1, 2, and 3, along with upstream interfaces of The Purdue Model, followed by a detailed risk analysis of each system and subsystem.
- Utilising methodologies like the ICS Cyber Kill Chain, incorporating real-world attacks and frameworks.
- Ensuring control and enablement objectives are directly derived from an analysis of business risks, with risk assessments tailored to the organisation's business drivers (i.e. The Business-Driven Principle).
- Prioritising the application of risk treatments and security measures to high-risk systems before addressing lower-risk areas, which is part of avoiding a one-size-fits-all approach to security control implementation.

Case Study



Global energy company sees the light with The Industrial Cyber Security Principle Method™

A large energy company with an international footprint came to SIS with a clear mandate to significantly modernise their approach to OT security, having been the target of increasingly sophisticated cyber threats in recent years.

We began with the actions that underscore our Business-Driven Principle to understand the OT environment within their operations and how this intersects with the way they do business. Interviews with OT managers were conducted to gain full transparency into their operations and culture, and to also ensure our OT recommendations accommodated the full spectrum of their requirements.

In conjunction with this organisational discovery, we performed a thorough risk assessment that looked at the security controls across the business. We assessed how these security controls were performing, how they could be refined to meet the demands of various subsystems across the company, and how they could be aligned to support their broader goals and strategic objectives. We combined this with our legacy and emerging knowledge of the utilities sector worldwide and its associated infrastructure.

This company's embracing of The Industrial Cyber Security Principle Method™––and specifically, our Business-Driven and Risk-Based recommendations––put them on a sure-footing to fortify their OT security posture.

3. Enterprise-Wide

The Enterprise-Wide Principle is about taking a whole-of-business perspective, right across every aspect of your organisation, to maximise the investment return and ensure the long-term value of your industrial cyber security.

Decisions made through an enterprise-wide lens ensure the time, effort and attention that goes into properly integrating your industrial cyber security into OT systems pays off in numerous ways. While OT may seem a very specific area of your business, it's one that can have huge ramifications across all your departments and operations, especially if there's a breach and/or your OT cyber security has been mismanaged.

OT/ICS integration goes beyond ticking off items on a ‘laundry list’.

Effective OT defences need multiple critical layers with various interdependencies to ensure sufficient protection. The laundry list method of ticking off industry-standard technical and procedural controls always falls short, mainly due to isolating each security control or focusing too narrowly on specific areas. A comprehensive approach that views all security controls as a cohesive unit working in harmony creates a robust, multi-layered defence system.

Another aspect to bear in mind is the relationship between IT and OT.

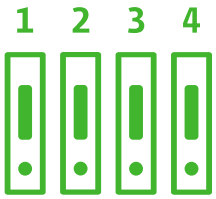
Taking a cross-enterprise perspective helps you see how any breakdown between IT and OT groups can lead to major cyber vulnerabilities. To prevent this occurring, employees in these departments need to effectively communicate and reconcile their (sometimes competing) priorities, even if this requires enlisting a third-party OT security specialist to facilitate these discussions. This is crucial for encouraging a unified approach to your organisation’s cyber security.

Operating in silos only exacerbates security risks.

Imposing one group’s processes on the other is another way to produce security debacles. Despite the differences in roles–whether corporate or plant/operational–all employees are integral members of the same team and must collaborate to safeguard the organisation.

Key actions for; The Enterprise-Wide Principle

- Adopting a consistent enterprise-wide perspective for all your industrial security decisions.
- Gradually securing enterprise-wide representation in decision-making processes and obtaining endorsement and support from senior management.
- Ensuring both IT and OT groups are synchronised with a common vision and mission for OT security.
- Designing industrial cyber security services that encompass a broad range of OT sites, covering all levels of The Purdue Model.
- Centralising all security mechanisms, products and technologies into management administration zones, where possible.



4. Methodical

The Methodical Principle is about approaching your OT cyber security in a meticulous and systematic manner. This relies on knowing the correct sequence of actions to take for optimal effectiveness of your OT.

Many organisations attempt to comply with multiple methodologies and standards at the risk of everything falling into a ‘muddy’ mess. A lack of refinement in implementation can be a major obstacle to achieving world-class security outcomes.

Interpreting industry methodologies is no easy feat.

Industry compliance standards are known to work but are also confusing in their complexity, especially for anyone inexperienced with implementing them. Without seasoned OT security specialists to lead the implementation, your organisation's industrial cyber security can fall seriously short of expectations.

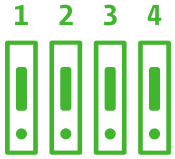
Drawing from a combination of standards offers the greatest value.

The best results come from knowing the ins & outs of the multiple methodologies and frameworks, and then using a combination of them all to meet the OT requirements of your specific business.

Organisations often search for a quick fix or 'silver bullet' but the harsh reality is no single solution fits all situations. By recognising this, along with the specialised expertise needed to safeguard your most valuable assets, you're placed in a strong position to ensure your OT is as secure as possible.

Key actions for; The Methodical Principle

- Developing teams with enhanced application experience and expertise in industrial cyber security standards.
- Refining your OT security methodology by investing strategically and creating an execution plan that implements security measures zone by zone.
- Crafting a comprehensive implementation plan that includes a business transformation and readiness assessment, along with processes for measuring and evaluating the maturity of your security implementations over time.
- Regularly reviewing all available industrial cyber security standards to acquire new insights and understand the advantages of a multi-standard approach for effective integration.



Case Study

Transport company finds the mortar in their security brickwork

A nationwide transport company had undergone a series of acquisitions that left their operations fragmented and their OT vulnerable. As part of a process to fully align the merged businesses into one, they partnered with SIS to bring together the IT and OT teams across the business, identify where responsibilities may to identify where responsibilities might be fragmented or disjointed, then introduce a methodical approach for securing their OT assets.

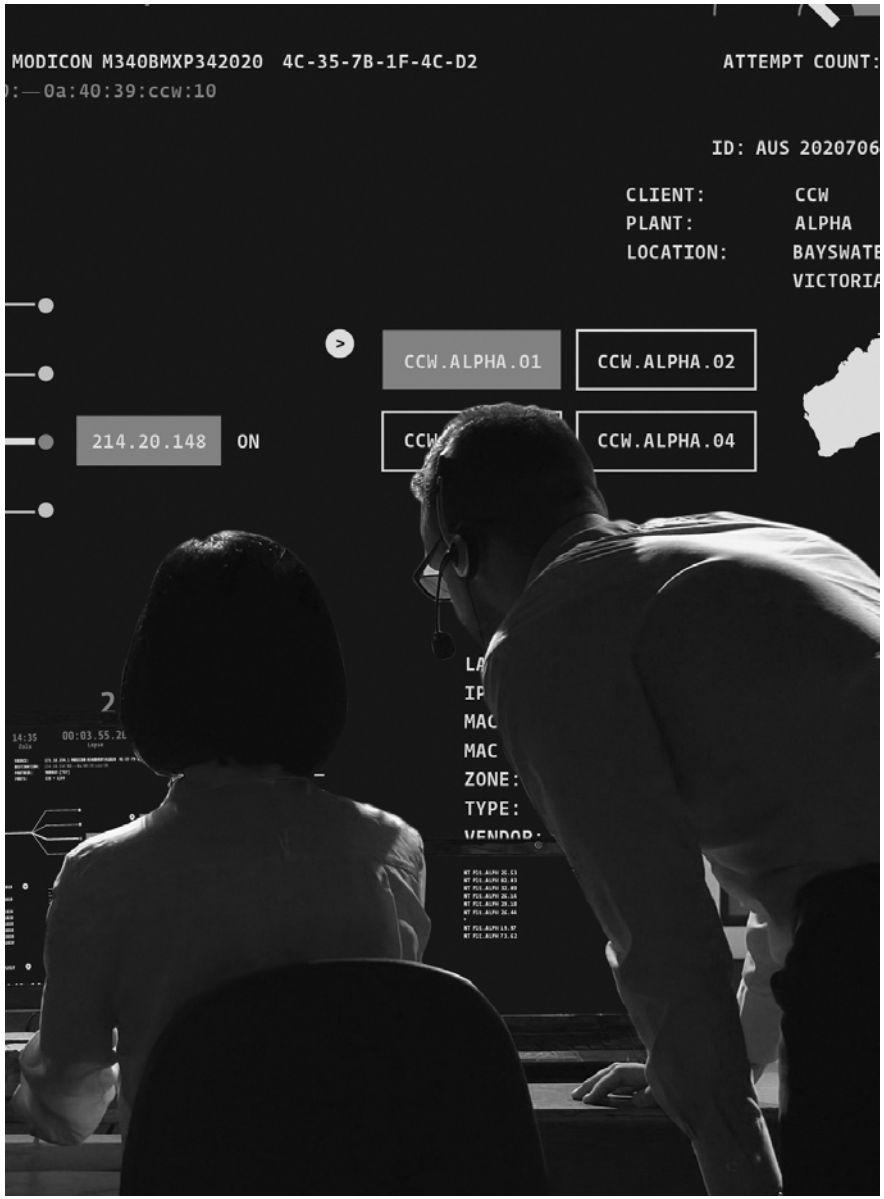
By addressing the needs of this company as a third-party OT cyber security specialist and deep diving into every aspect of their enterprise, we were able to pinpoint where the vulnerabilities in their OT lay, as well as the means for creating a unified approach that addressed any schisms across their organisation. We then methodically introduced our recommendations into their operations, while functioning as an intermediary between departments and personnel who had once struggled to communicate effectively.

Their partnership with SIS meant this freight and goods carrier could redefine themselves as a newly integrated entity. Most importantly, our engagement with them meant all relevant parties were now speaking the same language when it came to securing their critical operational infrastructure.

5. OT Security-Focused

The OT Security-Focused Principle is about recognising and maintaining the importance of your OT. This means using specialist OT security teams that strictly adhere to industry-specific standards and certification.

Introducing a 100% laser-focused industrial cyber security approach will help keep your organisation at the forefront of the current and developing cyber threat landscape. It's unlikely you can do it internally. Engaging external OT security specialists to unite with your internal team in adopting industry-specific security standards and certifications is ultimately the way to go.



Legacy constraints could be holding you back.

Systems that cannot support the implementation of technical automated security mechanisms or components – due to legacy constraints, system fragility, end-of-life status or compatibility issues – should have suitable compensating controls designed and implemented. These controls need to be customised for specific targets and developed through remediation plans created with your organisation's key stakeholders.

Not everything hinges on technology.

Although technology is crucial, the success of OT security often rests not on the technology itself but on bridging gaps between expectations, expertise and the individuals within an organisation. Effective training of your people is only possible when conducted by specialists who are deeply knowledgeable about OT security. Given the rapidly changing nature of OT security, staying updated with the latest practices and developments something you shouldn't have to shoulder.

The significance of aligning the right people formula and skills cannot be underestimated. After all, it is the people within the organisation who are deeply invested in OT and who bear the consequences when security measures fail.

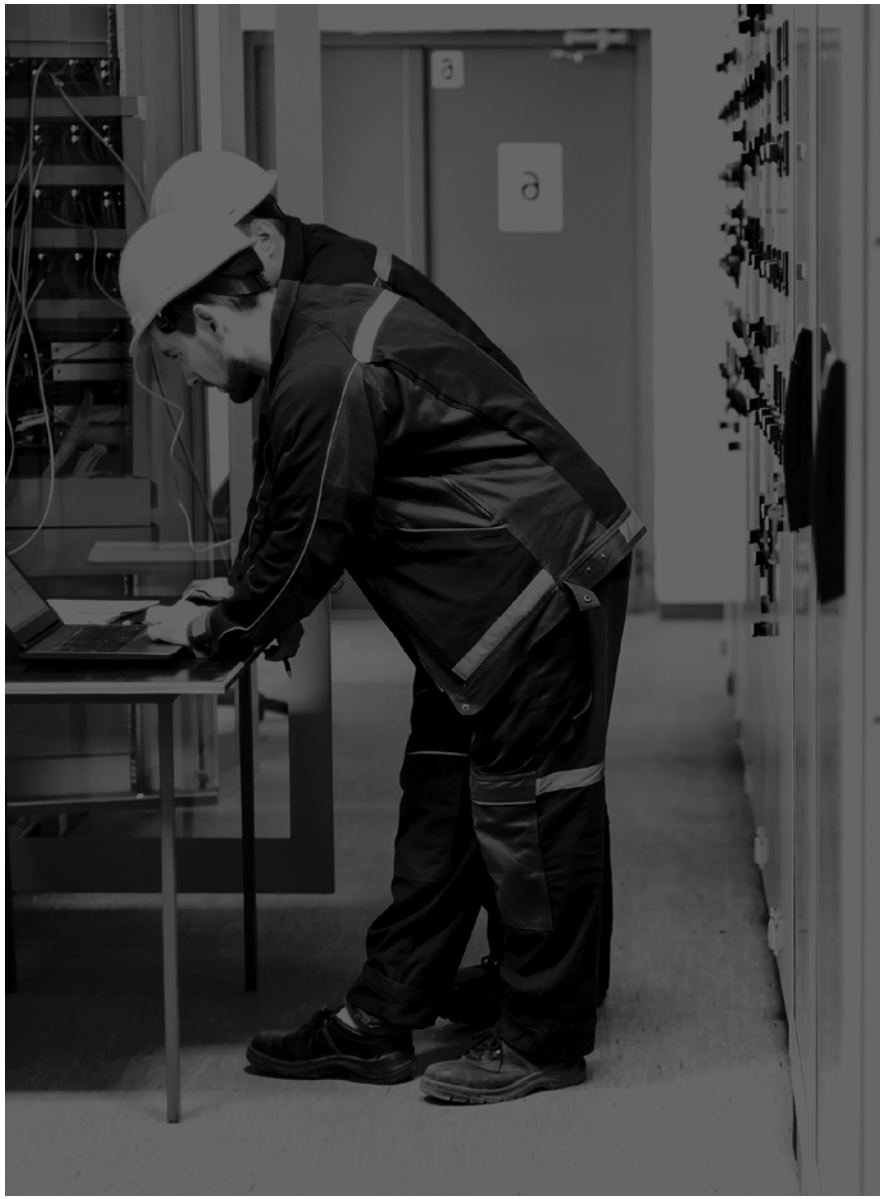
Key actions for;
The OT Security-Focused Principle

- Maintaining a 100% dedicated focus on OT security, avoiding an IT-centric approach to security control design and implementation that does not account for OT's unique business requirements.
- Conducting OT security assessments and audits at Levels 1, 2, 3, and upstream interfaces of Purdue model, adhering to specific industrial cyber security standards.
- Pursuing recognised certifications that confirm your compliance with OT security standards and protocols.
- Ensuring all OT users receive regular, targeted training in industrial cyber security.

6. OT Security-Compliant

The OT Security-Compliant Principle is about ensuring your organisation achieves and maintains compliance with the necessary regulatory frameworks governing OT – and then goes even further to give you the very best industrial cyber security.

If you're OT security-compliant, this means you hit the minimal recognised targets for adequately securing your industrial assets. The process usually involves registering OT assets, reporting cyber incidents affecting essential services and adhering to mandated risk management programs. It's a no-brainer for meeting your obligations.



More than a legality, it's a matter of principle(s).

The collective principles of The Industrial Cyber Security Principle Method™ directly inform your OT cyber security compliance in a highly organised way – so organised that the OT Security-Compliant Principle goes beyond industry expectation. As well as meeting your legal requirements, this combination of principles addresses the crucial factors that take your OT security from compliant to world-class industrial cyber security.

Non-compliance with critical OT security regulations and guidelines is a no-no.

If you're yet to achieve compliance, act immediately – you need to address compliance gaps and ensure adherence to industry regulations to properly mitigate risks. This is a situation where no excuses can be tolerated. But another point: you shouldn't rest on your laurels either. Being compliant is not a protective shield, so you need to go the extra mile to meet the idiosyncrasies of your specific business

Key actions for;
The OT Security-Compliant Principle

- Prioritising a Business-Driven and Risk-Based approach in your security strategies as a priority.
- Recognising that mere compliance does not guarantee best-in-class industrial security, other crucial factors must also be considered.
- Promoting voluntary adherence to OT security frameworks & standards established by regulatory bodies.
- Developing specific OT security incident response plans to enhance preparedness.
- Acting proportionately according to the security implications and the severity of any non-compliance.
- Maintaining consistent interactions with regulators as required.

Case Study

Mining company makes good on its OT security mantra

A base and precious metals mining company was well aware of the ramifications of insufficient OT cyber security but were grappling with realising their infrastructure security vision. Given this company's round-the-clock operations, any halt to production – no matter how minimal – could potentially cost them millions of dollars, so protecting their critical assets was top of mind.

After working through the principles of The Industrial Cyber Security Principle Method™, they noted a lack of in-house skills to fully protect and monitor their OT, so opted to enlist SIS for a complete implementation and management of a dedicated OT-Security Operations Centre (SOC) that actively protects their critical assets through expert monitoring and analysis of any threats or events targeting OT systems and devices.

By treating their OT with the security-focus it deserves, this metals mining company has accelerated their security posture with voluntary compliance to leading industry OT security standards.

See how your organisation stacks up against the benchmark

The Industrial Cyber Security Principle Method™ is a methodology rather than a step-by-step process. It acknowledges the prevailing aspects that need to be incorporated into any OT security approach and that should remain apparent at all times.

While it is not dogmatically prescriptive, The Industrial Cyber Security Principle Method™ is proven to work as a methodological response to today's OT cyber threats and allows for the specific details of different organisations to be written into its story.

Would you like to find out how you benchmark against The Industrial Cyber Security Principle Method™?

Take the test yourself at scorecard.ics-sis.com and see how you shape up.