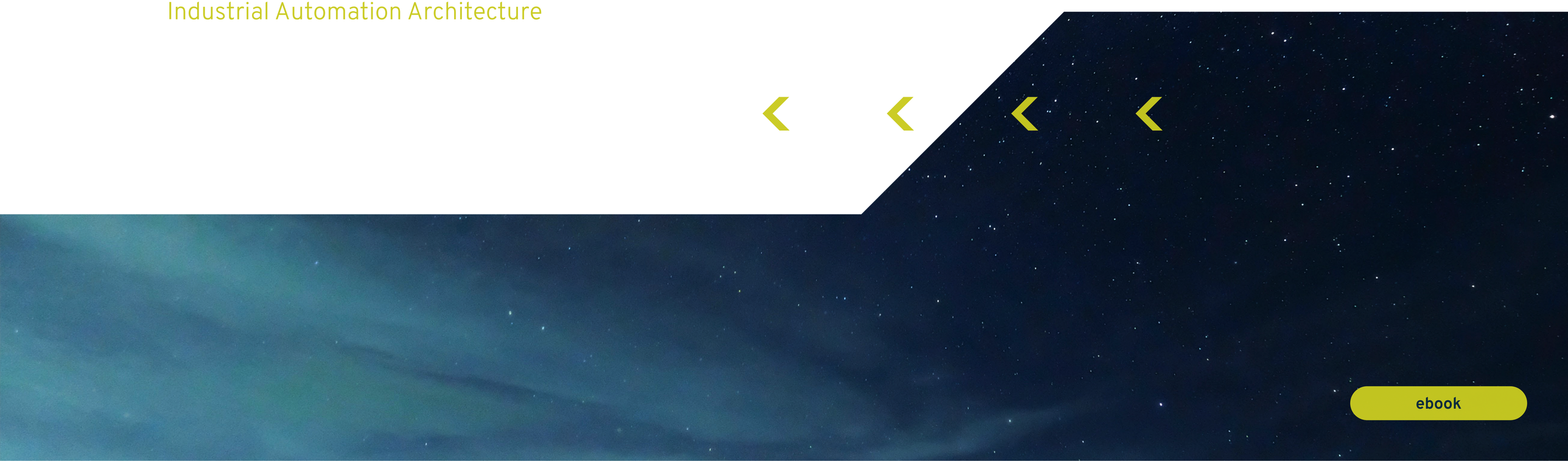
IriusRisk

Securing operational technology infrastructure

A Guide to Comprehensive Threat Modeling for Industrial Automation Architecture



ebook

IriusRisk

Digital transformation is enabling the introduction of new and emerging operational technologies.

The critical infrastructure for many large corporations is moving away from traditional methods of process control, implementing emerging operational technologies and cloud infrastructure so processes no longer need to be controlled locally.

This shift and the adoption of cloud technology increases the productivity and stability of industrial control systems and allows engineering teams access to fault monitoring, maintenance requirements and alarm systems remotely – improving scale, productivity and overall efficiency.

Although industrial automation through Edge computing and emerging operational technology opens the door to fast, productive and cost-efficient operations, it also introduces additional vulnerability points to systems and the network itself that need to be covered.

Why threat modeling is important in industrial automation

The International Electrotechnical Commission (IEC) has recently introduced the IEC 62443 set of standards developed specifically to secure Industrial Automation and Control Systems (IACS) which currently includes nine standards, technical reports (TR) and technical specifications (TS). These were developed to overcome the inadequacy of existing IT standards that are deemed inappropriate for important and critical national infrastructure systems and processes.

IEC 62443 takes a risk-based approach to cyber security, which is based on the concept that it is neither efficient nor sustainable to try to protect all assets in equal measure. Instead, users must identify what is most valuable and requires the greatest protection and identify vulnerabilities.

In order to meet the requirements of Part 3 of the standard in particular, threat modeling has been identified as a significant methodology in building cyber resilience within IACS.

IriusRisk

Security across your architecture

Using Edge computing for process control devices means using public networks to transfer data to the cloud – information that that can be sensitive which corporations do not want to land in the wrong hands.

The threat of cyberattacks on devices is also present, with the potential of a successful breach leading to disabled networks, data theft and operations grinding to a halt. With potentially hundreds of devices in use across large organizations, security becomes a multi-department challenge, not just for IT.

Security is paramount in all modern ICS architectures, and there are several factors that come into play that must be considered by organizations when deploying security measures such as threat modeling.

01.

Speed to market

The tangible benefits that modern process control brings often leads to corporations seeking to put them into practice quickly. The design, development, testing, commissioning and implementing of projects that would take six years are now under pressure to be completed in three.

The pressure to get solutions up and running faster often has a knock-on effect on security, with devices being put into live networks that are not configured correctly, software and hardware that isn't robust, and code that isn't secure.

IriusRisk

Ease of use

For threat modeling to be effective, it needs to be implemented throughout the software development lifecycle (SDLC) and be used confidently by Architectural, Development and Security teams. Their ideal goal is for the threat modeling process to be intuitive and so well embedded in the SDLC that they do not even have to think about it. The easier the threat modeling solution is to use, the easier this can be achieved.

02.

03.

Connected collaboration

The ability to collaborate between teams, in person or remotely, throughout the threat modeling process is a key factor when choosing a solution. Organizations want a seamless experience across their Architecture, Development and Security teams.

IriusRisk

Valuable expertise

Given that automated, scalable threat modeling is a relatively new area of security within industrial automation, a supportive and experienced threat modeling provider can close secure design gaps and work on long term continuous security improvements.

04.

Adopting a start left approach

If security flaws and design errors are not identified until after an application goes into testing, corrections can be expensive, both in resources and in time invested. The National Institute for Standards and Technology (NIST) has estimated that correcting code once an application is in production can take thirty times the time required for remediation and re-design.

As a result, there has been a move towards adopting a start left approach—one that starts earlier on in the development cycle. Automated threat modeling at design time is an activity recommended by the NIST[1] and the OWASP[2] to ensure that engineering teams build adequate security controls into a product.

The key to scaling this activity across a large portfolio of applications is to move the responsibility for software security from the central security to the engineering teams and to empower those teams with a self-service automated threat modeling solution. This removes the central security team as a bottleneck to the product release process, allowing faster releases that still meet the security and compliance requirements of the organization.

[1] https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/recommended-minimum-standard-vendor-or-developer

[2] https://owasp.org/Top10/A04_2021-Insecure_Design/

IriusRisk

What is threat modeling?

Modern threat modeling has moved on from manual processes. It doesn't wait until the application goes into production. Instead, it takes place in the design phase of a system or application and automates the process of threat modeling throughout the Software Development Lifecycle (SDLC), subsequently accelerating the time to market and dramatically reducing the cost of re-design. Current authorities class it as being an essential part of application design:

01.

The OWASP Top Ten calls for increased use of threat modeling, particularly when dealing with the problem of insecure design, listed as the fourth most critical security risk to applications.

02.

NIST references it as the first step in their Recommended Minimum Standard for Vendor or Developer Verification of Code.

03.

Gartner places it within the ASRTM (Application Security Requirements and Threat Management) category.

IriusRisk

How to build a threat model

Organizations want threat modeling to be easy to use for everyone, and to be so well embedded in the development cycle that there's no need to even think about it.

One typical way of building an embedded threat model is based on the basic principles of Adam Shostack's four-question scheme. This model allows the user to detect security deficiencies during the design phase of the application.

IriusRisk

01.

Build
the diagram

What are we building?

02.

Pinpoint
the threats

What can go wrong?

03.

Identify
the mitigations

What are we doing to protect ourselves against the threats?

04.

Validate
the model

Did we do a good job?

Validate steps 1-3.

Document the process.

A successful Threat Modeling tool will:

- Be a single point of management for the security team. This allows them to work with an updated view of the risks within their portfolio
- Use automation to generate security requirements based on the application architecture model and the relevant standards
- Have enough flexibility to adopt either industry-specific risk models or customized security policies based on a pre-regulatory triage
- Establish a two-way communication with the Application Lifecycle Management (ALM) tools that the development teams use
- Enable API access that allows automation
- Allow dynamic updates to the risk model and implementation strategy
- Integrate with the main security tools used throughout the development cycle
- Generate a visual diagram of the architecture that can act as an active document for the stakeholders

IriusRisk

Bring change to life

Implementing a security program that includes threat modeling involves a cultural and organizational change rather than a technical change.

IriusRisk

01.

Start with a pilot project that applies only to a specific set of applications to confirm there are enough resources and support to make the end result a success. Any threat modeling tool should be collaborative. This involves explaining what will take place, why it will benefit each stakeholder and what the overall effect will be.

02.

Organizational change must always be communicated, even when the project is a pilot. Adapt the corporate development procedures to include threat modeling once the application architecture is defined to make sure your project succeeds. Understanding how averse to risk the business is in relation to each application is essential to creating a risk-based security strategy. A threat modeling tool helps you manage resources more efficiently so you can make better decisions.

IriusRisk

Finally, Security Champions should remember that security requirements are not exclusively their preserve. The requirements should be published, challenged, improved and adapted to the agreed business risk appetite and regulatory compliance needs.

Undertaking a threat modeling strategy offers significant business benefits. Not only does it present a demonstrable ROI, but it's also not a complex activity to undertake. Threat modeling underpins other types of security testing, reviewing and auditing, and increases the productivity of business processes. It also improves time to market and instills an appetite for security all the way up to the C-suite.

The alternative?
Do nothing and cross the corporate fingers until the organization has no choice but to act.

IriusRisk

Introducing IriusRisk - proactive software security by design

Secure doesn't have to be slow. By partnering with IriusRisk, you'll have the support of our easy-to-use automated threat modeling platform to help you identify architectural security flaws before you start building.

The IriusRisk platform can be delivered either as an on-premises solution or through SaaS. Powerful, scalable and collaborative, it's designed to help your engineering and security teams identify architectural security flaws during design, saving you time, avoiding delays and accelerating your time to market by baking security earlier into your development process.

IriusRisk

Automated threat modeling

IriusRisk helps you beat the complexity of manual threat modeling with its powerful automation engine, providing a reliable self-service tool for designing secure applications that's simple for your engineers to use.

Security starts with design

Half of today's software flaws are in the design. Our platform lets you generate threat models in minutes, along with recommended and required countermeasures and specific, actionable advice for your engineering teams.

A smart investment

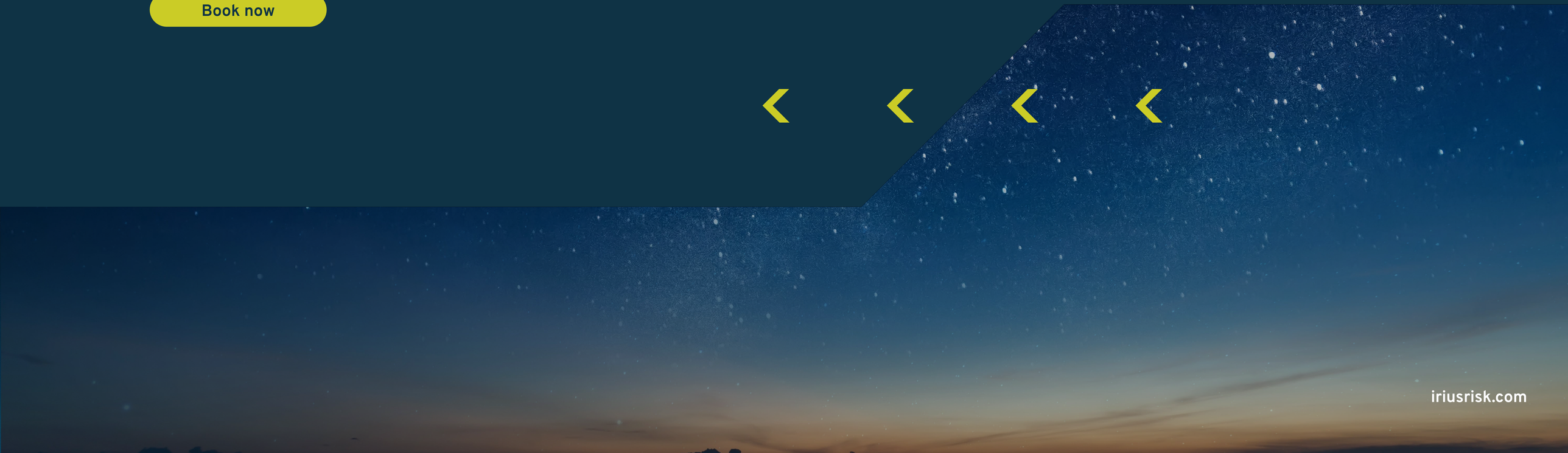
Smart threat modeling requires smart, targeted investments. Know how much to invest in security and where to invest it to get maximum return on your investment.

IriusRisk

Experience our platform first-hand

Book a consultation with our threat modeling specialists to see the tangible benefits that IriusRisk can deliver for your business.

Book now



iriusrisk.com