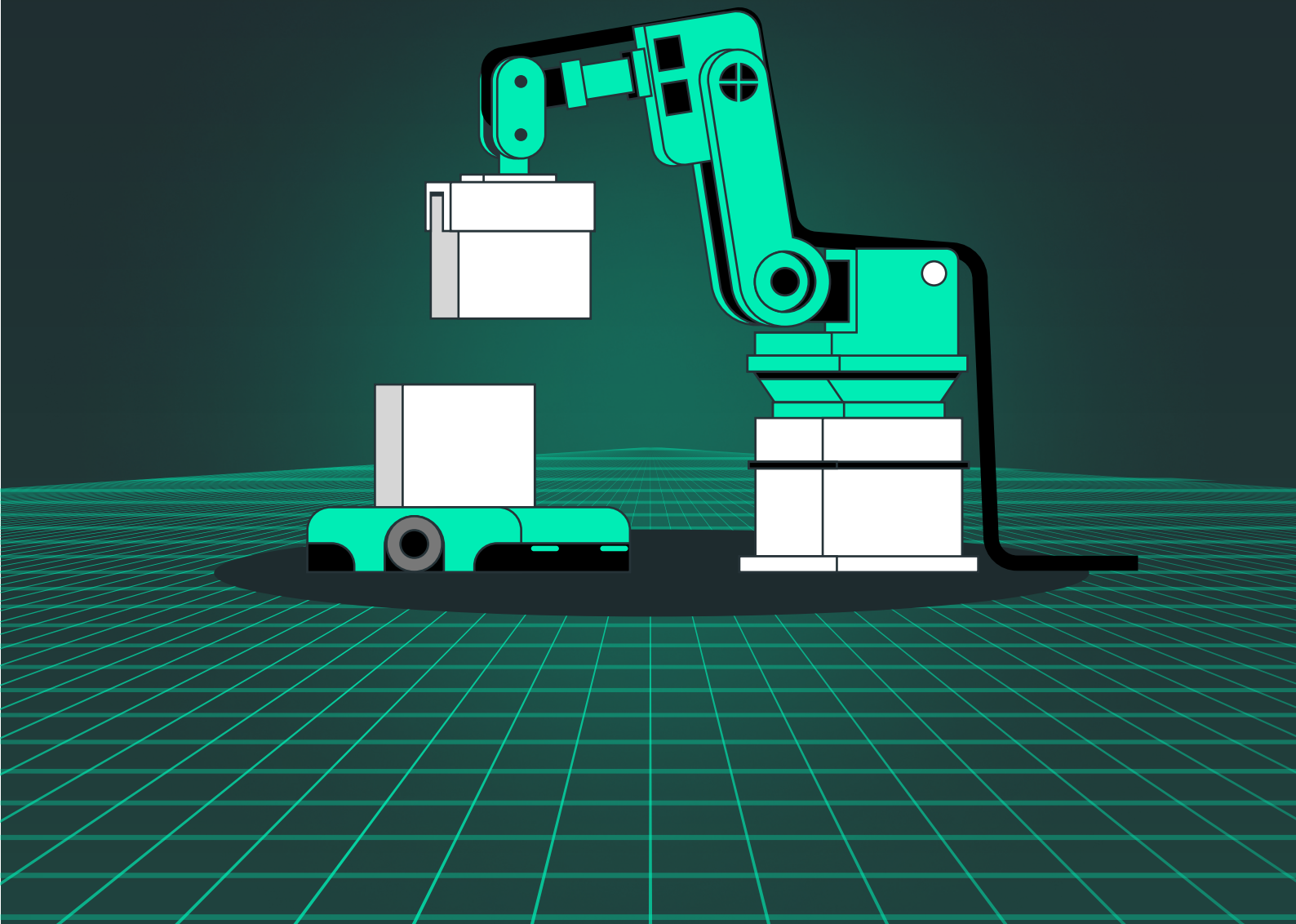
IriusRisk

Securing operational technology infrastructure eBook

A Guide to Comprehensive Threat Modeling for Industrial Automation Architecture



Setting the scene for Operational Technology

Critical infrastructure for many large corporations is moving away from traditional process control technology. The adoption of cloud technology increases the productivity and accessibility of industrial control system elements and allows engineering teams remote access to monitoring, maintenance cycles and alarm/safety systems – improving scale, productivity and overall efficiency.

Although industrial automation through Edge computing and Industry 4.0 emerging operational technology opens the door to fast, productive and cost-efficient operations, it also opens the attack surface to systems with vulnerabilities.

Enter the era of artificial intelligence (AI) and the potential vulnerabilities and entry points for an attack magnify beyond the norm. While AI can increase productivity and automation, with it comes unique risk. Industrial automation remains a lucrative target for causing exponential damage within essential production lines for health, manufacturing, oil and gas, and more.

Frameworks and Standards for Industrial Automation

This industry already has the International Electrotechnical Commission (IEC) IEC/ ANSI 62443 set of standards developed specifically to secure Industrial Automation and Control Systems (IACS). And now, MITRE has released MITRE EMB3D for 2024, a comprehensive framework designed to safeguard embedded devices used in industries like healthcare, automotive, and critical infrastructure.

More about IEC 62443

IEC/ ANSI 62443 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. It has been added to over more recent years.

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 4-2 of the standard in particular, threat modeling has been identified as a significant methodology in building cyber resilience within IACS.

More about MITRE EMB3D

The framework will be updated when necessary with new vulnerabilities and defenses, ensuring it stays relevant as security risks evolve over time.
EMB3D helps organizations to prioritize security investments and take the appropriate steps to mitigate them.

It provides a structured model that identifies potential cyber threats, maps them to specific device properties, and suggests mitigation strategies.

Three key benefits include:

- **Improved security posture** - aids organizations to proactively address vulnerabilities in embedded devices. Increasing security and reducing the likelihood of breaches.
- **Regulatory and compliance alignment** - mapped to widely used standards such as IEC/ANSI 62443, simplifying compliance and reducing audit burdens and effort.
- **Real-time security** - the framework will be adapted to respond to emerging threats, ensuring systems remain protected against the most current threats - as and when they arise.

Why threat modeling matters

The threat of cyberattacks on devices is continuously 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.

There are several factors that come into play that must be considered by organizations when deploying proactive security measures such as threat modeling:

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 and 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.

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.

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.

Valuable expertise

Given that automated, scalable threat modeling is still an emerging 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.

What exactly is threat modeling?

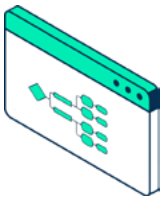
Threat modeling is a repeatable way of assessing the security of your architecture, quantifying your level/ likelihood of risk, and concluding with actionable countermeasures to mitigate those risks. Find out more in this blog ' What is threat modeling and how does it work?'

NIST references it as the first step in their Recommended Minimum Standard for Vendor or Developer Verification of Code. Gartner places it within the ASRTM (Application Security Requirements and Threat Management) category. 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.

Adopting the Four Question Framework

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.

The four questions are:



1. What are we working on?

2. What can go wrong?

3. What are we going to do about it?

4. Did we do a good enough job?

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

How to build a threat model

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

Bring change to life

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.

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.

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.

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.

Introducing IriusRisk - providing secure by design across your products and services

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.

AI-Augmented and automated threat modeling

IriusRisk helps you beat the complexity of manual threat modeling with its powerful automation engine, and in-built AI Assistant, 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.

Integrations across your existing tech stack

You don't have to start from scratch thanks to our open API and prebuilt bidirectional workflows with popular tools like Jira, Zervicenow, Azure DevOps and many more.

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, and your unique industry.

Automate Threat Modeling to fit your existing SDLC

Secure design right from the start

Visit **www.iriusrisk.com**

to book your demo

IriusRisk