spOT™
Securing the Digital Machine Lifecycle
for Machine Builders

An OTORIO E-Book

OTORIO

Table of Contents

A Changing Machine Building Ecosystem

Today's Machine Building ecosystem extends far beyond the Factory Acceptance Test. Keeping the security of your machines in-line with customer policies, best practices, warranty requirements and regulatory demands remains your responsibility - long after they're working on your customer's production floor.

With machines comprising tens of components from multiple vendors, today's Machine Builders are effectively a long-term part of the end-product supply chain. This is a game changer. Because today, product responsibility, risk and (especially) liability doesn't end until end of product life.

Rapidly Evolving Supply Chains

Machine builders by definition serve clients who are also vulnerable to cyberattack. As we learned from the Solarwinds, Codecov and most recently Kaseya attacks, threats to the manufacturing supply chain – in which machine builders play a major role – are serious, real, and rapidly-growing.

The reason? Even as manufacturers invest heavily in the cybersecurity of their own networks, hackers have begun turning their focus towards highly-complex Machinery product ecosystems, which themselves rely on a complex supply chain. Because even if Machine builders have the best security measures in place, they still depend on hundreds of downstream components that can be exploited by attackers.

The fact is that once machines are delivered, machinery supply chains become the end customer's supply chains, too.

Rethinking Machinery Cybersecurity

Machine builders need to ensure that each machine is secured and compliant before delivery. Already, manufacturers are asking for proof of such security and compliance – and builders need to be ready to quickly perform automated checks and provide auditable reports during Site Acceptance Testing (SAT).

Machine manufacturers also need to verify that their machines are aligned with industry best practices, customer security and other policies, warranty and service requirements, as well as constantly-evolving international and local regulations. And they need to proactively notify customers upon discovery of new vulnerabilities, providing clear remediation guidelines in real or near-real-time.

Despite this, until recently it was nearly impossible to identify, track and mitigate vulnerabilities on every machine at every customer - including every on-board asset from every vendor.

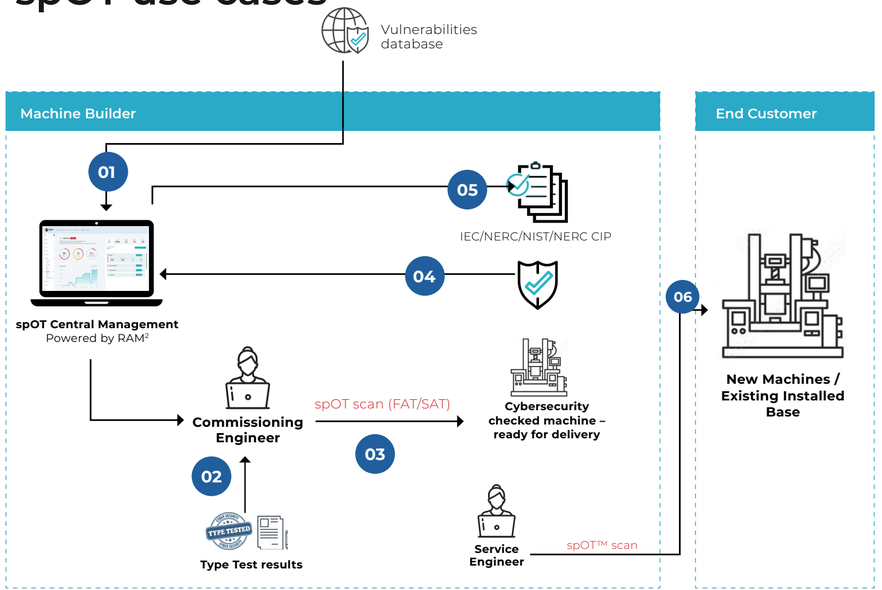
That’s why OTORIO developed spOT™

OTORIO’s spOT ensures secure and compliant machinery – from the single asset to the entire manufacturing site. spOT empowers machine builders to automate machine security assessments and significantly reduce the time and costs of FAT/SAT processes. In addition, it allows machine manufacturers to continue managing the machine’s cybersecurity posture throughout its entire lifecycle on customer premises.

Powered by OTORIO’s RAM² platform, spOT conducts an enriched asset inventory of every machine at every customer site. Then, it automatically assesses new and existing systems – scanning thousands of assets across multiple products and sites, and correlating with vendor updates and OTORIO’s security intelligence database. And when a cybersecurity vulnerability is identified, spOT identifies the exact machines affected by it - and notifies Product Security teams so they can improve the product compliance and alert their customers.

OTORIO’s spOT™ allows machine manufacturers to continue managing the machine’s cybersecurity posture throughout its entire lifecycle on customer premises.

spOT use cases



01 Automatic update of spOT™ with latest known vulnerabilities

02 Commissioning Engineer uses spOT™ type-test results + predefined type test parameters data set as basis for cyber security FAT test

03 Run spOT™ test scan (FAT/SAT) and generate finger-print for each delivered machine

04 Transfer fingerprint dataset into machine builders spOT™ central management

05 Automatically generates compliance report for each machine

06 Service Engineer uses spOT™ scan + already stored type-test and runs gonging cyber security test (remote or on-premise)

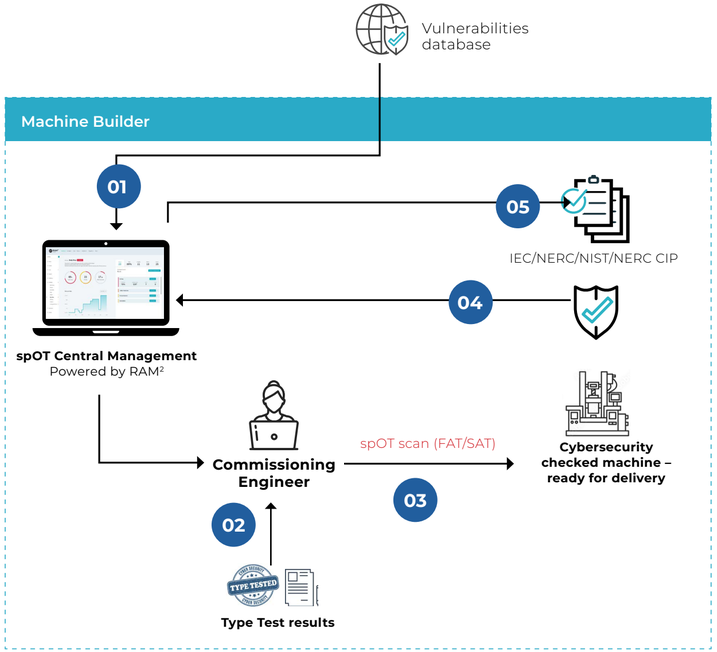
spOT Use Cases

01.

Secure and Compliant Machines Delivery

During the Factory Acceptance Test (FAT), spOT conducts an on-demand scan of each machine - online or offline. It identifies all the assets comprising each machine – hardware and software. Then, it maps vulnerabilities and compliance gaps against known CVEs, as well as OTORIO's proprietary databases. The end result is a detailed cybersecurity and compliance report that delivers an in-depth risk assessment for pre-delivery machines.

During customer Site Acceptance Testing (SAT), spOT automatically verifies cyber protection and compliance before the machine is connected to the customer production line. spOT scans and analyzes machines in their new ecosystem, checking how interaction with the new environment impacts security. Eliminating the need for time and resource-intensive manual mapping, spOT dramatically lowers the costs associated with SAT.



01 Update spOT™ with latest known vulnerabilities

02 Commissioning Engineer uses spOT™ type-test results + predefined type test parameters data set as basis for cyber security FAT test

03 Run spOT™ test scan (FAT/SAT) and generate finger-print for each delivered machine

04 Transfer fingerprint dataset into machine builders spOT™ central management

05 Automatically generates compliance report for each machine

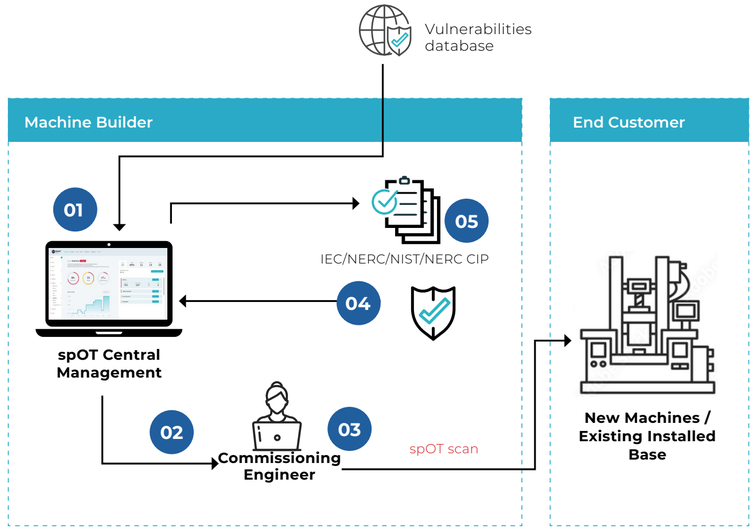
spOT Use Cases

02.

Cybersecurity-as-a-Service

spOT opens new business opportunities for machine builders enabling them to offer value-added post-delivery cybersecurity services - ensuring their machines stay cyber-resilient until end of life. spOT's periodic or on-demand cybersecurity and compliance checks can be performed remotely or on-prem. spOT identifies new vulnerabilities throughout each machine's lifecycle and automatically alerts customers.

spOT allows machine builders to alert customers in real time of changes in machine security posture. spOT can alert when new vulnerabilities are discovered that may affect assets within machines already in the field, or when a machine's configuration is altered, for example after maintenance.



01 Automatic update of spOT™ with latest known vulnerabilities

02 Service Engineer uses spOT™ scan + already stored type-test and runs ongoing cyber security test

03 Test could be handled via remote connection or directly on premise with spOT™ scan

04 Store updated fingerprint dataset in machine builder's spOT™ Central management

05 Automatically generates compliance updated report for each machine

Why spOT?

FAT check for every machine / delivery

Becomes part of the machine delivery and quality procedures

- Supports system hardening
- Checks the full machine against the relevant IEC62443 / NIST / NERC CIP / or additional standards as required requirements
- Creates Cyber Security “machine fingerprint” for further business opportunities
- Generates automatically the machine specific IEC compliance letter

Lifecycle Vulnerability Management As-a-Service

- Based on the “fingerprint” of delivered machines, spOT™ periodically checks these configurations against current threats and vulnerabilities.
- Cyclic cyber security risk potential evaluation of end customer machineries as a machine builder service

About OTORIO

OTORIO designs and markets the next generation of OT security and digital risk management solutions. The company combines the experience of top nation-state cybersecurity experts with cutting edge digital risk management technologies to provide the highest level of protection for the critical Infrastructure and manufacturing industry.

Visit our website: www.otorio.com

Visit our website: www.otorio.com