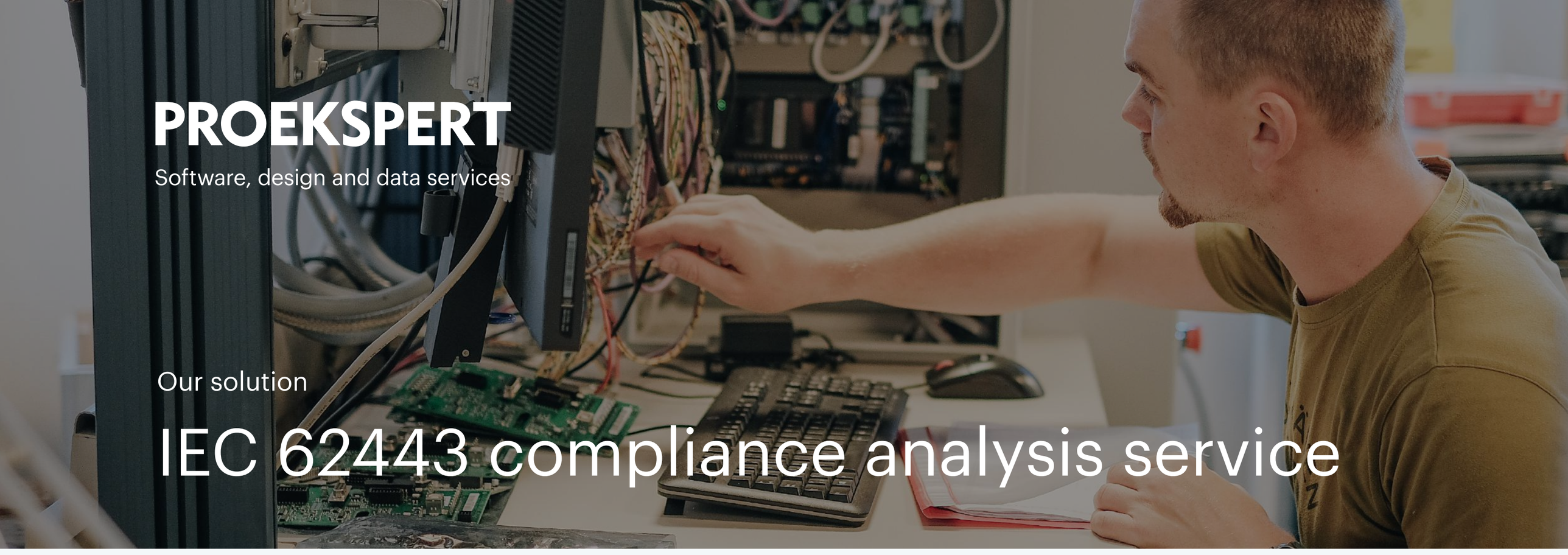

PROEKSPERT

Software, design and data services

Our solution

IEC 62443 compliance analysis service

Scale your product reach

Innovate with balanced product cost

Reduce product maintenance costs

Proekspert helps device manufacturers prepare for the EU Cyber Resilience Act (CRA). One big part of the CRA Act is introducing cybersecurity rules for manufacturers and developers of products with digital elements, covering both hardware and software.

Many companies conduct cybersecurity audits to get a better overview of their current situation. Proekspert offers self-assessment or third-party assessment services to industrial device manufacturing companies as they prepare for IEC 62443 certification.

Why Proekspert

Many companies conduct cybersecurity audits to get a better overview of their current situation. Proekspert offers self-assessment or third-party assessment services to industrial device manufacturing companies as they prepare for IEC 62443 certification.

Key features and benefits of our service

We help industrial device manufacturing companies with self-assessment or third-party assessment needed in the process of preparing for IEC 62443 certification.

We help identify and map product development processes and vulnerabilities

We also help suggest security measures to mitigate security risks in your product source code or in the development process

What is IEC 62443

IEC 62443 is an international series of standards that address cybersecurity for operational technology in automation and control systems. The standard describes both technical and process-related aspects of automation and control systems cybersecurity. The purpose of the standard is to help suppliers, system integrators, and manufacturers comply with process requirements and to address security concerns along the supply chain.

Before certification, an assessment must be conducted. There are two possibilities: (1) **self-assessment** and (2) **third-party assessment**.

How it works

To assess current state of cybersecurity for operational technology in automation and control systems we follow:

IEC-62443-4-1

Requirements for development processes

IEC-62443-4-2

Requirements for product/component

IEC-62443-3-3

Requirements for systems

Tools we use for the IEC 62443 compliance analysis:

Threat model visualization to identify cyber security threats (STRIDE methodology)

Security risk structuring to classify exploits and attack vectors (Mitre ICS Matrix)

Software composition analysis to identify and manage **open-source** components and **potential security vulnerabilities** in code (Polaris Black Duck)

Static analysis of product source code to detect and **fix code defects** and ensure code quality and security (Polaris Coverity Scan)

Services

Proekspert provides industrial device manufacturing companies with self-assessment or third-party assessment needed in the process of preparing for IEC 62443 certification.

- Identifying and mapping product development processes and vulnerabilities
- Suggesting security measures to mitigate security risks in product source code or in the development process

Results of the assessment services:

- Factual input for product strategy
- Mapped processes
- Mapped vulnerabilities

Get in touch

Our experienced engineers can help assess cyber risks concerning your product. Let's see if we are the right partner for you.

Terry London

Partner & Product Manager

terry.london@proekspert.ee

Terry London

Phone: +372 651 8700

Read more about this solution on our website:

proekspert.com/iec-62443-compliance-analysis-service