



WHITE PAPER EN 50742

Cybersecurity in Machinery Directive Engineering: Time Savings and Legal Compliance under the New EN 50742

How machinery manufacturers utilize the new SaaS product **EnCo ASE** (AI-powered Safety & security Engineering) to conduct automated **THREAT ASSESSMENT** threat assessments and ensure compliance with the EU Machinery Regulation.

1. Executive Summary

The ongoing connectivity in machinery and plant engineering (Industry 4.0, IoT, remote maintenance) opens up immense economic opportunities – but also introduces critical cyber risks. With the new EU Machinery Regulation (MVO) 2023/1230 and the harmonized standard **EN 50742** ("Protection of machinery against corruption"), responsibilities are shifting fundamentally: IT security is no longer an optional feature, but a mandatory requirement for CE marking.

Manufacturers face the challenge of conducting complex threat assessments without blocking existing safety processes or tying up immense human resources.

This white paper demonstrates how **EnCo Software GmbH** provides a solution to seamlessly integrate threat assessments in accordance with **EN 50742** using the software platform EnCo ASE and its dedicated **THREAT ASSESSMENT** module.

The result: Maximum time savings through automated workflows and absolute legal compliance during audits.

2. The Regulatory Challenge: EN 50742 & Machinery Regulation

Traditionally, machinery safety focused primarily on classic safety (e.g., **EN ISO 12100**) to protect humans from the machine. The new **EN 50742** looks in the opposite direction (security): It regulates the protection of safety-related control systems against intentional or unintentional corruption (manipulation) via digital access.

The Problem in Practice:

- **Complexity:** The standard requires seamless identification of interfaces, assets, and cyber threats throughout the entire lifecycle of the machine.
- **Tool Fragmentation:** Assessments are often painstakingly maintained in isolated Excel spreadsheets. This leads to errors, inconsistencies, and high maintenance efforts.



- **Liability Risk:** Without a valid threat assessment and proof of the required Safety-Related Security Level (SRSL), companies face the risk of losing CE compliance and suffering severe penalties in a worst-case scenario.

3. The Solution: The **THREAT ASSESSMENT** Methodology in EnCo ASE

To identify threats systematically, the **THREAT ASSESSMENT** model has become firmly established. It analyzes systems based on six attack vectors:

Abbreviation Threat		Meaning in Machinery Engineering (Example)
S	Spoofing	Identity theft (e.g., unauthorized access to the maintenance interface)
T	Tampering	Manipulation of data or parameters of the safety control system
R	Repudiation	Ability to deny actions (lack of logging for modifications)
I	Information Disclosure	Data exposure (unauthorized retrieval of recipes or operational data)
D	Denial of Service	Disruption of services (paralyzing emergency stop communication in the network)
E	Elevation Privilege	of Gaining rights (a user unauthorizedly obtains admin privileges)

The **THREAT ASSESSMENT** module of **EnCo ASE** translates this methodology directly into the machinery engineering workflow. Instead of starting from scratch, the module docks directly into the existing system model (e.g., from the System Designer).

4. Dual Added Value for Users

Legal Compliance at the Touch of a Button

- **Compliance by Design:** EnCo ASE guides the user step-by-step through the process required by EN 50742 – from asset identification to defining countermeasures to achieve the appropriate SRSL (Safety-Related Security Level).



- **Audit-Proof Documentation:** Evaluations and reports are generated automatically. In the event of an inspection by authorities or certification bodies (such as TÜV or DGUV Test), the comprehensive documentation baseline is instantly available.
- **Revision Security:** Thanks to integrated versioning and baseline management, every change remains traceable and consistent.

Massive Time Savings in Engineering

- **No Duplicate Data:** The THREAT ASSESSMENT module is fully integrated into the EnCo ASE workbench. Safety analyses (such as FMEA, FTA, HARA) and security analyses (TARA / THREAT ASSESSMENT) share the exact same database. Changes to system components are automatically applied across all analyses.
- **Automated Threat Mapping:** Based on the defined interfaces (e.g., USB, cloud, fieldbus), the software automatically suggests typical THREAT ASSESSMENT threat patterns. This eliminates time-consuming brainstorming sessions.
- **Frictionless Collaboration:** Teams work simultaneously on a central platform. The time-intensive consolidation of different Excel files is completely eliminated.

5. Conclusion & Outlook

The implementation of EN 50742 must not become an innovation roadblock for machinery manufacturers. Continuing to analyze digital threats with makeshift tools wastes valuable development time and risks compliance gaps.

With **EnCo ASE** and the dedicated **THREAT ASSESSMENT module**, companies transform a regulatory obligation into an efficient standard operating procedure. The seamless integration of safety & security drastically minimizes engineering overhead, shortens time-to-market, and guarantees maximum legal compliance for the future of machinery engineering.

About EnCo Software GmbH

Founded in 2008 and headquartered in Hamburg, **EnCo Software GmbH** is a leading provider of integrated software solutions in the field of Functional Safety and Cybersecurity.

The flagship platform SOX supports companies worldwide in developing highly complex, safety-critical systems efficiently, compliantly, and sustainably.

The product SOX, which has been on the market since 2012, is currently being succeeded by EnCo Software GmbH's new SaaS platform, **EnCo ASE. Ready for EN 50742?**

[Schedule a free EnCo ASE demo](#) and experience the **EnCo ASE EN 50742 THREAT ASSESSMENT Module** live in action.