



EU-Maschinenverordnung & Cyber Resilience Act mit minimalem Aufwand erfüllen

Externe Best Practice für Risikoeinschätzung und Dokumentationspflicht erfüllen, erforderliche Schutzmaßnahmen minimieren. Ohne eigenen Kompetenzaufbau.

Executive Summary

Mit zunehmender Vernetzung entstehen für Maschinenhersteller neue Cybersecurity-Anforderungen. Die EU-Maschinenverordnung (EU) 2023/1230 und der Cyber Resilience Act (EU) 2024/2847 verlangen, entsprechende Risiken künftig systematisch zu bewerten und zu berücksichtigen. Für viele Unternehmen bedeutet das neuen zusätzlichen Prüf- und Dokumentationsaufwand sowie das Risiko unnötiger Schutzmaßnahmen.

Hydrive ermöglicht es, die neuen Anforderungen vollständig zu erfüllen und den zusätzlichen technischen Aufwand auf ein Minimum zu begrenzen. Dazu werden die konkreten Cybersecurity-Risiken bewertet und aufgezeigt, wo wirklich Handlungsbedarf besteht. Komponentenseitig vorhandene Schutzfunktionen werden gezielt genutzt, zusätzliche Maßnahmen nur dort entwickelt, wo sie tatsächlich notwendig sind.

Das Ergebnis:

- ✓ Schnelle Klarheit über Risiken und Handlungsbedarf
- ✓ Entsprechung der geforderten Dokumentationspflichten
- ✓ Minimaler Eigenaufwand zur Entsprechung der gesetzlichen Anforderungen
- ✓ Kein eigener Know-how-Aufbau

Das Problem:

Herausforderung Cybersecurity-Pflichten

Functional Safety ist im Maschinenbau seit Jahrzehnten etabliert. Gefährdungen, die unmittelbar von einer Maschine ausgehen, werden bewertet und durch geeignete Schutzmaßnahmen auf ein vertretbares Maß reduziert – entsprechend den einschlägigen Vorschriften.

Mit zunehmender Vernetzung durch Funk- und Netzwerkschnittstellen, Remote-Services und Software-Updates entstanden jedoch neue Risiken. Diese wurden von den bisherigen Prüf- und Schutzmaßnahmen nicht abgedeckt.

Darauf reagieren die EU-Maschinenverordnung (EU) 2023/1230 und der Cyber Resilience Act (EU) 2024/2847. Cybersecurity-Risiken müssen künftig ebenfalls systematisch berücksichtigt werden.

Gerade kleinere und mittelständische Entwicklungsorganisationen stellt das vor erhebliche Herausforderungen. Das erforderliche Know-how ist häufig nicht vorhanden. Gleichzeitig entsteht zusätzlicher Aufwand: Neue Regelwerke müssen verstanden, technische Folgen bewertet und Entscheidungen belastbar dokumentiert werden – parallel zum Tagesgeschäft.

Hinzu kommt ein wirtschaftliches Risiko. Aus Unsicherheit können teure Schutzmechanismen entwickelt werden, die für die konkrete Maschine möglicherweise gar nicht erforderlich sind. Das belastet unnötig Verkaufspreis und Marge.

Die Lösung:

Externe TARA und pragmatische Schutzmaßnahmen

Durch mehrere parallele Kundenprojekte konnte Hydrive frühzeitig umfangreiche Expertise in der Anwendung der EU-Maschinenverordnung und des Cyber Resilience Acts aufbauen – speziell im Bereich Mobilmaschinen.

Daraus hat Hydrive eine klare Best Practice entwickelt: Anforderungen vollständig erfüllen – aber nur den technischen Aufwand betreiben, der tatsächlich erforderlich ist.

Bewährt hat sich dafür im ersten Schritt das aus der Automotive-Cybersecurity und der ISO/SAE 21434 bekannte Threat Analysis and Risk Assessment (TARA).

Hydrive bewertet dabei mögliche Angriffsflächen, deren potenzielle Auswirkungen und das daraus entstehende Risiko für die konkrete Maschine und ihr Umfeld. So wird transparent, wo tatsächlich Handlungsbedarf besteht. Im nächsten Schritt wird geprüft, wie sich erforderliche Schutzmaßnahmen mit möglichst geringem eigenem Aufwand umsetzen lassen. Dazu prüft Hydrive zunächst, welche Schutzfunktionen die eingesetzten Komponenten und Steuerungsplattformen bereits bieten.

So können vorhandene Funktionen wie sichere Update-Verfahren, Verschlüsselung, Zertifikate, Zugriffsbeschränkungen oder Secure Boot der eingesetzten Komponenten und Steuerungsplattformen bereits ausreichen, um identifizierte Sicherheitslücken zu schließen – ohne zusätzliche Eigenentwicklung.

Fehlen dennoch Funktionen, entwickelt Hydrive gemeinsam mit dem Kunden ein passendes Maßnahmenkonzept. Je nach Ausgangslage können bestehende Mechanismen ergänzt, Zugänge anders abgesichert oder bei älteren Steuerungsplattformen eine Modernisierung beziehungsweise Portierung geprüft werden.

Das Ergebnis: Die neuen Anforderungen werden schnell und nachvollziehbar erfüllt, Cybersecurity-Risiken zuverlässig begrenzt und zusätzliche Schutzmaßnahmen nur dort umgesetzt, wo sie tatsächlich erforderlich sind. So bleibt der Implementierungsaufwand auf ein Minimum begrenzt.

Problem	Hydrive Maßnahmen	Nutzen
Neue Pflichten, unklare Auswirkungen	Externe TARA / strukturierte Cybersecurity-Risikoanalyse	Entsprechung der Vorschriften, Klarheit über Risiken und Handlungsbedarf, kein eigener Kompetenz- und Ressourcenaufbau erforderlich
Offene Schnittstellen	Prüfung vorhandener Schutzfunktionen der eingesetzten Komponenten	Eigenentwicklung auf ein Minimum reduzieren
Hoher interner Aufwand	Hydrive Best Practice & technisches Sparring	Schnell zu belastbaren Entscheidungen ohne Eigenaufwand
Fehlende Schutzfunktionen	Pragmatisches Maßnahmenkonzept und ggf. Lean-Modernisierung	Gefordertes Schutzniveau mit minimalem Aufwand

Ihre Maschine prüfen – Risiken erkennen, Aufwand minimieren

Sie möchten die Safety- und Security Anforderungen für eine Ihrer Maschinen schnell und wirtschaftlich gemäß EU Maschinenverordnung und Cyber Resilience Act prüfen, dokumentieren und gegebenenfalls umsetzen?

Dann nutzen Sie die Expertise von Hydrive!

So geht es:

Schritt 1 – Erstgespräch

Wir zeigen Ihnen anhand konkreter Praxisfälle, wie Hydrive die Anforderungen bei vergleichbaren Aufgabenstellungen bewertet und mit möglichst geringem Umsetzungsaufwand erfüllt hat.

Schritt 2 – Vor-Workshop (virtuell)

Sie stellen Hydrive Ihren konkreten Anwendungsfall vor. Gemeinsam klären wir Ausgangslage, Herausforderungen und Zielsetzung. Anschließend erhalten Sie einen Vorschlag für das weitere Vorgehen.

Schritt 3 – Strukturierte Security-Risikobetrachtung TARA

Hydrive führt eine strukturierte Security-Risikobetrachtung durch und zeigt, wo konkreter Handlungsbedarf besteht. Sind zusätzliche Schutzmaßnahmen erforderlich, besprechen wir das ideale weitere Vorgehen.

Vereinbaren Sie jetzt ein kostenloses Erstgespräch:

JETZT TERMIN BUCHEN

Über Hydrive

Die Hydrive Engineering GmbH mit Sitz in Freital bei Dresden unterstützt seit fast 20 Jahren die Entwicklung energieeffizienter Maschinen und Anlagen – mit dem Ziel, den technologischen Vorsprung ihrer Kunden zu sichern und nachhaltige Lösungen wirtschaftlich umzusetzen. Das Unternehmen ist mit einem interdisziplinären Team aus 25 Spezialistinnen und Spezialisten in der gesamten DACH-Region aktiv.

Zu den Kunden von Hydrive zählen unter anderem Claas, Liebherr, Adenso und Sany. Das AUTOMATION-Framework, das aus der langjährigen Projektpraxis heraus entwickelt wurde, wird bereits von Unternehmen wie Liebherr, Adenso, Suffel, Sany und Reiss erfolgreich eingesetzt. Es entlastet Entwicklungsabteilungen, standardisiert komplexe Abläufe und beschleunigt die Umsetzung moderner Automatisierungslösungen.

Jetzt unverbindlich mehr erfahren

Sie möchten die Safety- und Security-Anforderungen für eine Ihrer Maschinen schnell und wirtschaftlich gemäß EU-Maschinenverordnung und Cyber Resilience Act prüfen, dokumentieren und gegebenenfalls umsetzen? Dann lassen Sie uns unverbindlich sprechen!

Vereinbaren Sie jetzt Ihr kostenloses Erstgespräch.

JETZT TERMIN BUCHEN

Direktkontakt

Dr. Thomas Neubert, Geschäftsführer
tne@hydrive.gmbh



Hydrive Engineering GmbH
Dresdner Straße 172
01705 Freital bei Dresden
Deutschland

Tel: +49 351 850 731 0
E-Mail: info@hydrive.gmbh
Web: www.hydrive-engineering.de