Vorwort

Warum 2027 das entscheidende Jahr für Maschinenhersteller ist

2027 ist der neue „TÜV-Termin“ für deine CE-Welt. Ab dem 20. Januar 2027 zählt nur noch die neue Maschinenverordnung (EU) 2023/1230 – und Ausreden mit „alte Richtlinie“ funktionieren nicht mehr, nicht vor den Behörden und im Streitfall nicht vor Gericht. Die Übergangsphase ist dann vorbei.

Was das konkret bedeutet: Wer bis dahin seine Hausaufgaben nicht gemacht hat, steht mit einer fertigen Maschine da – aber ohne Marktzugang. Die Überwachungsbehörde nimmt die alte Richtlinie nicht mehr an. Der Importeur kann deine Maschine nicht anmelden. Der Betreiber darf sie nicht in Betrieb nehmen (rechtlich). Und wenn doch was passiert, haftest du nicht nur technisch – du haftest auch rechtlich dafür, dass du die neue Verordnung ignoriert hast.

Die gute Nachricht: Das ist kein Hexenwerk. Es ist Handwerk – nur eben mit neuen Regeln. Wer jetzt anfängt, ist 2027 lieferfähig. Wer wartet, muss im Januar 2027 improvisieren. Und ich kann dir jetzt schon sagen: Das wird richtig teuer.

Das Kernproblem, das die Verordnung lösen soll: Die alte Maschinenrichtlinie von 2006 stammt aus einer Welt, in der Maschinen überwiegend mechanisch waren. Software war selten, Vernetzung noch seltener, KI unbekannt. 2027 ist das ganz anders. Heute hat jede etwas größere Maschine einen Computer, spricht mit dem Internet, bekommt Updates. In einer vernetzten Produktion sprechen Maschinen mit Maschinen (Industrie 4.0). Die alte Verordnung war für diese digitale Welt nicht gemacht. Daher wurde sie aktualisiert.

Warum ich dieses Buch geschrieben habe – und wem ich dafür danke

Dieses Buch ist für diejenigen, die 2027 nicht überrascht sein wollen. Es ist für Konstrukteure, die verstehen müssen, was sich ändert – nicht nur in Theorie, sondern in der täglichen Arbeit am CAD und in der Risikobeurteilung. Es ist für Geschäftsführer, die wissen wollen, was es kostet, wenn sie zu spät handeln: Umkonstruktion, verzögerte Markteinführung, Haftungsrisiken, die sich nicht einfach wegversichern lassen. Es ist für Juristen und Compliance-Manager, die die neuen Anforderungen greifbar brauchen – nicht als abstrakte Norm, sondern als praktischer Kompass für den Alltag. Und es ist für Betreiber und Integratoren, die verstehen müssen, welche Konsequenzen die neue Verordnung für ihre Maschinenflotten hat.

Entstanden ist dieses Buch nicht im luftleeren Raum. Es basiert auf Jahren der Erfahrung als öffentlich bestellter und vereidigter Sachverständiger, auf Gefährdungs-

beurteilungen in der Praxis, auf Haftungsfällen, die ich analysiert habe, und auf Diskussionen mit Ingenieuren und Unternehmern, die genau diese Fragen stellen.

Mein besonderer Dank gilt Peter Oberstein, der mich mit kritischem Blick, tiefem Fachwissen und wertvollen Diskussionen bei diesem Projekt begleitet hat. Seine Fragen und Perspektiven haben dieses Buch geschärft und authentischer gemacht. Ohne seine tatmächtige Unterstützung und seine unermüdliche Bereitschaft, auch schwierige Fragen zu durchdenken, wäre dieses Werk nicht das geworden, was es ist.

Der „elektrotechnische" Dank gebührt *Wolfgang Fink* mit seinem gewaltigen Normenwissen und deren Kombination mit viel praktischem und vor allem gesundem Menschenverstand. Er ist mein elektrotechnisches „Gewissen" seit vielen Jahren. Danke *Wolfgang*!

Die EU-Verordnung 2023/1230 ist kein Überfall – sie ist eine Antwort auf eine veränderte Welt. Eine Welt, in der Maschinen intelligenter werden, in der Cybersecurity genauso wichtig ist wie mechanische Sicherheit, und in der die alte Trennung zwischen Hardware und Software aufgelöst ist. Genau darum geht es in den folgenden Kapiteln: Verstehen, was sich ändert. Wissen, was es bedeutet. Und vor allem: Handeln, bevor es zu spät ist.

Die nächsten Monate bis Januar 2027 sind deine Chance – nutze sie.

Cyber trifft Safety: Die neue Realität für VEFK und Sicherheitsfachkräfte

Früher war die Welt noch in Ordnung. Du hast die Schutztür geprüft. Funktioniert? Haken dran. Du hast den Not-Halt geprüft. Reagiert? Haken dran. Du hast den Lichtvorhang getestet. Reaktionszeit passt? Haken dran. Fertig. Die Sicherheitsfunktionen waren mechanisch und elektrisch. Sie waren lokal. Sie waren nicht erreichbar von außen.

Das war gestern. Definitiv gestern!

Heute musst du auch das Netzwerk dahinter ernst nehmen. Die Schutztürlogik läuft in einer Sicherheits-SPS, die übers Ethernet erreichbar ist. Der Not-Halt wird digital ausgelöst, und das Signal läuft übers Netzwerk. Der Lichtvorhang wird per Firmware aktualisiert, und die Firmware muss signiert sein. Cyberangriffe sind die neuen „unsichtbaren Schraubendreher" im Schaltschrank, und nur weil sie unsichtbar sind, sind sie nicht weniger real.

Die zentrale Erkenntnis: Ein Hacker kann heute die gleichen Schäden anrichten wie ein Mensch mit Schraubendreher, der ungehindert Zugang zu deiner Arbeitsstätte hat. Er kann Parameter manipulieren. Er kann Logiken verändern. Er kann malicious Firmware einspielen, die den Überstromschutz abschaltet. Der einzige Unterschied zu früher: Der Hacker sitzt einen Kontinent entfernt und wird selten erwischt.

Die andere Variante ist, dass der Übeltäter Gehalt bekommt. Ein Großteil der manchmal unabsichtlichen Angriffe auf Netzwerke kommt von Insidern. Die müssen nicht einmal bösartig sein. Es reichen Nachlässigkeit, Dummheit und Unwissenheit, um Schaden anzurichten. Ich denke an die Mitarbeiter, die den USB-Stick, den sie auf dem Parkplatz gefunden haben, in den USB-Port ihres Rechners stecken, einfach weil auf dem Stick „Gehälter" stand.

Wer Safety denkt, ohne Cyber mitzudenken, lässt mindestens eine Seitentür offen. Und genau vor diesen Seitentüren warnt die neue Maschinenverordnung der EU. An dieser Stelle möchte ich auf das Buch „Cybersicherheit und die Elektrofachkraft" (VDE-Schriftenreihe 210) aus dem VDE VERLAG verweisen. Unter „Cyber" darf man nicht nur die IT-Sicherheit verstehen, sondern auch die Elektrosicherheit und die Arbeitssicherheit. Denn diese können in der betrieblichen Praxis nur im Dreiklang funktionieren.

Das ist kein reines IT-Thema. Und das ist der Grund, warum wir mit diesem Buch Elektrotechniker, nicht IT-Security-Spezialisten ansprechen – weil ihr das verstehen müsst, ihr seid die, die es prüfen müsst.

Für wen dieses Buch ist (Hersteller, Betreiber, Elektrofachkräfte, Sicherheitsverantwortliche)

Dieses Buch richtet sich an alle, die am Ende den Kopf hinhalten: Konstrukteure, die die Maschine designen. Elektrotechniker (EFK), die sie bauen. Sicherheitsfachkräfte (VEFK), die sie prüfen. Betreiber, die sie betreiben. Und Geschäftsführer, die nachts nicht schlafen, weil sie wissen, dass eine Haftung auf sie wartet.

Also an alle, die wissen wollen: **„Was muss ich konkret tun, damit meine Maschine 2027 noch laufen darf – und ich ruhig schlafen kann?"**

Dieses Buch ist nicht akademisch. Es ist nicht „juristisch überfrachtet" (bei Bedarf kann ich dir tolle Anwälte nennen). Und es ist nicht über Vorschläge und Regeln, die du nicht praktisch umsetzen kannst. Es ist handwerklich.

Wo die Fallen sind

Dieses Buch nimmt dich mit durch die konkrete Welt deiner Maschinen – nicht in abstrakte Risikokataloge, sondern in echte Szenarien, die du erkennst, weil du sie vielleicht selbst schon erlebt hast oder bei Konkurrenten siehst. Du wirst verstehen, wo die Fallen lauern: bei der Fernwartung, die plötzlich ein Cybersecurity-Risiko ist. Bei den Betriebsdaten, die der Betreiber sammelt, ohne zu wissen, dass die Verordnung das jetzt anders bewertet. Bei den Updates, die über das Internet kommen und die alte Sicherheitslogik durchbrechen. Nicht als akademische Risikomatrizen, sondern als das, was in deiner Fabrik oder in der des Kunden tatsächlich passiert.

Die Maßnahmen, die ich dir zeige, sind nicht die IT-Security-Verfahren aus dem Silicon Valley oder von Großkonzernen – das ist für dich nicht 1 : 1 umsetzbar. Sondern ich erkläre dir, wie ein Elektrotechniker diese Anforderungen versteht, wie er sie prüfen kann, und wie er sie in die bestehende Sicherheitslogik einordnet, die er ohnehin schon beherrscht. Das ist die Sprache von Messinstrumenten, Schaltplänen und prüfbaren Zuständen – nicht von kryptografischen Protokollen.

Die Dokumentation ist ein Kapitel, das viele Hersteller hassen, weil sie es als Bürokratie sehen. Aber das ist falsch verstanden. Die Dokumentation ist deine Waffe im Ernstfall – wenn etwas schiefgeht, wenn ein Betreiber eine Maschine falsch nutzt, wenn die Behörde nachfragt, wenn es vor Gericht kommt. Deine Dokumentation ist das, was dir den Rücken freihält. Sie zeigt, dass du gedacht hast. Dass du die Risiken gekannt hast. Dass du gehandelt hast. Wer das nicht aufschreiben kann, haftet auch für das, das er nicht tun konnte – einfach, weil er nicht nachweisen kann, dass er es versucht hat.

Wie du es gegenüber Behörden und vor Gericht argumentierst, das ist im Schadensfall dann die Frage, die dich am meisten interessiert. Vertraue nicht auf Glück und schöne Worte. Das geht mit Struktur, mit nachvollziehbaren Entscheidungswegen und mit einer Dokumentation, die zeigt, was du getan hast und warum. Mit Fachkompetenz, die sichtbar wird – nicht unbedingt, weil du alles perfekt gemacht hast, sondern weil du es redlich versucht hast und das nachweisen kannst.

Die knallharte Botschaft am Ende: 2027 ist nicht der Untergang des deutschen oder europäischen Maschinenbaus. Es ist nicht das Ende eines Geschäftsmodells. Es ist einfach ein neuer Standard – wie die Maschinenrichtlinie 2006 einer war, wie CE-Kennzeichnung einer war. Das Umsetzen von Maßnahmen kann Maßstäbe können erlernt werden. Und wer das jetzt tut, hat in zwei Jahren einen echten Wettbewerbsvorteil: klare Prozesse, sichere Maschinen, dokumentierte Verantwortung, und vor allem: Marktzugang ohne Drama.