

# Retrofit & Maintenance

# 2025

**Technische  
Logistik**

Hebezeuge  
Fördermittel

Grundlagen | Projekte | Unternehmen





# Cybersecurity in der Intralogistik

Neue EU-Vorgaben und wie Automatisierungsspezialisten heute schon Antworten liefern

**Automatisierte Intralogistik-Anlagen gelten als Rückgrat moderner Produktions- und Distributionsprozesse. Sie ermöglichen eine präzise, schnelle und effiziente Abwicklung innerbetrieblicher Materialflüsse. Doch mit der zunehmenden Digitalisierung dieser Systeme wächst auch ihre Verwundbarkeit – insbesondere gegenüber Cyberbedrohungen. Die Europäische Union hat darauf reagiert und mit der neuen Maschinenverordnung (EU 2023/1230), dem Cyber Resilience Act (EU 2024/2847) sowie der NIS-2-Richtlinie einen neuen Ordnungsrahmen geschaffen, der auch Betreiber und Inverkehrbringer automatisierter Anlagen in die Pflicht nimmt.**

Ab dem Jahr 2027 wird es für Unternehmen in der Intralogistik nicht mehr ausreichen, ihre neugebauten Anlagen lediglich mechanisch instand zu halten. Vielmehr sind dann ganzheitliche Sicherheitsstrategien gefordert, die auch Software, Kommunikationstechnik und vernetzte Infrastrukturen einbeziehen. Für viele Betreiber bedeutet das eine grundlegende Umstellung. Gleichzeitig ergeben sich Chancen für Automatisierungsspezialisten wie Unitech: Sie können Verantwortung übernehmen und Kunden dabei unterstützen, die neuen Anforderungen zu erfüllen, indem sie progressive und weitsichtige Serviceangebote bereitstellen.

## Regulatorischer Umbruch: Was sich ab 2027 ändert

Die neue EU-Maschinenverordnung löst die bisherige Maschinenrichtlinie ab und definiert erstmals explizit Anforderungen an die Cybersicherheit von Maschinen und Anlagen. Damit wird anerkannt, dass moderne Maschinen häufig softwarebasiert arbeiten, mit Netzwerken verbunden sind und über digitale Schnittstellen verfügen. Herstellende Unternehmen – und in vielen Fällen auch Betreiber – sind künftig verpflichtet, digitale Risiken bereits in der Entwurfsphase zu berücksichtigen. Ebenso verlangt die Verordnung, dass auch bei Softwareänderungen, beispielsweise durch die Integration neuer Funktionen oder Softwareupdates, eine erneute Risikobewertung durchgeführt werden muss. Ergänzt wird dies durch den Cyber Resilience Act, der branchenübergreifend verbindliche Anforderungen an die Sicherheit digitaler Produkte definiert. Für Anbieter von Maschinen mit digitalem Kern, wie etwa Lagerverwaltungssoftware oder Automatisierungskomponenten, bedeutet dies unter anderem die Pflicht, sichere Grundeinstellungen ab Werk zu gewährleisten, Schwachstellen (beispielsweise durch verwendete Drittanbieterprodukte) offenzulegen und auf empfohlene Sicherheitsupdates hinzuweisen. Darüber hinaus verlangt die NIS-2-Richtlinie von sogenannten „wichtigen Einrichtungen“ ein professionelles Risikomanagement in der Informationssicherheit, inklusive Meldepflichten bei Sicherheitsvorfällen.

**800**

**relevante Normen**

müssen noch entsprechend angepasst und harmonisiert werden.

All dies führt zu einer tiefgreifenden Veränderung in der Betreiberverantwortung. Wer eine automatisierte Intralogistikanlage betreibt, muss nicht nur deren Verfügbarkeit und Leistung sicherstellen, sondern auch ihre digitale Resilienz dauerhaft gewährleisten. Dazu gehören Maßnahmen wie Patchmanagement, Zugriffskontrolle, Protokollierung, sichere Updateverfahren und ein kontinuierliches Monitoring. Diese Anforderungen sind kein einmaliger Akt, sondern verlangen organisatorische, personelle und technische Veränderungen über den gesamten Lebenszyklus einer Anlage hinweg.

Auch wenn der grobe regulatorische Rahmen bereits festgelegt wurde, gibt es für die Gremien der EU-Kommissionen noch viel Detailarbeit zu erledigen. Bis zum Inkrafttreten von Maschinenverordnung und Cyber Resilience Act müssen noch etwa 800 relevante Normen entsprechend angepasst und harmonisiert werden. Das stellt eine große Herausforderung für Hersteller und Inverkehrbringer dar, die heute eine langfristige Lieferverpflichtung eingehen, aber auch für die mittelfristige Planung der Betreiber.

### Die Betreiberperspektive: Herausforderungen und Verantwortungsverschiebung

Für Betreiber von Bestandsanlagen stellt sich insbesondere die Frage, wie sie diesen neuen Vorgaben gerecht werden können, ohne dabei laufende Prozesse zu gefährden oder hohe Investitionen tätigen zu müssen. Denn viele Anlagen sind über Jahre gewachsen, wurden modular erweitert und basieren auf Software- und Hardwareständen, die nicht mehr dem aktuellen Stand der Technik entsprechen.

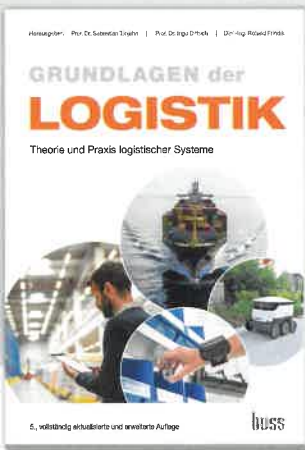
Ein weiteres Problem ist die unklare Trennung zwischen Hersteller- und Betreiberpflichten. Wenn Betreiber eigenständig Softwareänderungen vornehmen oder Komponenten austauschen, können sie unter Umständen rechtlich als „neuer Inverkehrbringer“ gelten und müssen allen damit verbundenen Pflichten der CE-Konformität nachkommen. Die Einbindung von Drittanbietern, etwa im Rahmen von Fernwartung oder Cloud-Anbindungen, erhöht die Komplexität zusätzlich.

Hier wird deutlich: Betreiber benötigen Partner, die nicht nur technische Expertise mitbringen, sondern auch in der Lage sind, regulatorische Anforderungen zu übersetzen und in konkrete Maßnahmen zu überführen. Genau an diesem Punkt setzt Unitechnik mit seinen Leistungen an.

Regelmäßige Sicherheitsupdates für Betriebssysteme, Datenbanken und Laufzeitumgebungen werden strukturiert geplant, getestet und in Abstimmung mit dem Kunden ausgerollt.



UNITECHNIK



## Unverzichtbares Grundwissen Logistik

Das Fachbuch „Grundlagen der Logistik“ hat sich mittlerweile als Standard-Werk etabliert.

Mit der 5. Auflage 2022 setzen die Autoren das bewährte Konzept fort, den Leser schrittweise an das Thema Logistik heranzuführen und einen Überblick über die wichtigsten Anwendungsgebiete zu geben. Die einzelnen Schwerpunkte der Logistik sind in komprimierter Form von namhaften Autoren der jeweiligen Fachgebiete dargestellt. Darüber hinaus behandelt das Grundlagenwerk vertieft neue Themen wie **Nachhaltigkeit/Green Logistics**, **Qualitäts-, Umwelt- und Risikomanagement**, **Dokumentenlogistik**, **Reverselogistik** und **Urban Retail Logistics**.

Paperback, Format DIN A4, 500 Seiten, 300 Abb. und Tab.

Bestell-Nr. 22603 € 92,- | ab 10 Stück à € 84,- | ab 25 Stück à € 78,-

E-Book Best-Nr. 226039 € 73,74

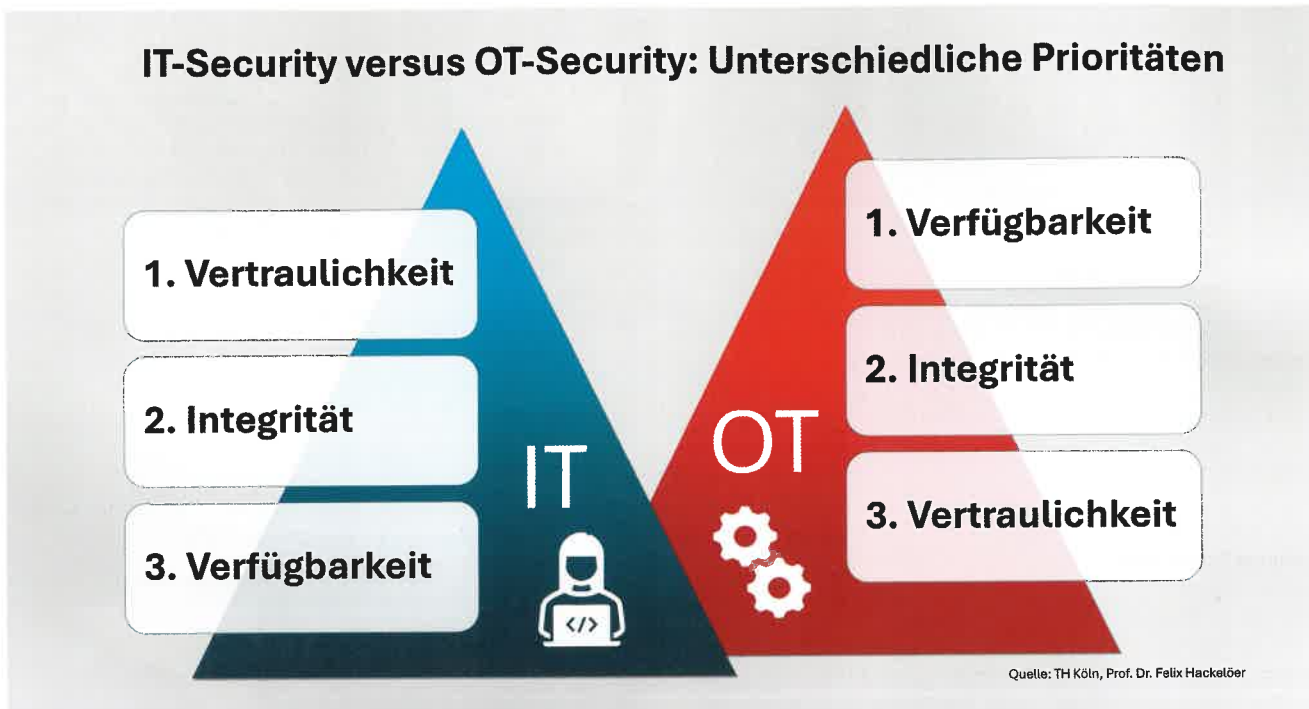
Preise freibleibend zzgl. MwSt. und Versand. Es gelten die Lieferbedingungen der HUSS-VERLAG GmbH unter [www.huss-shop.de](http://www.huss-shop.de).



HUSS-VERLAG GmbH · 80912 München  
Tel. +49 (0)89/323 91-317 · Fax -416  
[shop@hussverlag.de](mailto:shop@hussverlag.de)

[www.huss-shop.de](http://www.huss-shop.de)

IT-Security schützt klassische Unternehmens-IT, während OT-Security sich auf die Absicherung von industriellen Steuerungs- und Automatisierungssystemen bezieht.



## Sicherheit als Service – am Beispiel Unitechnik

Unitechnik unterstützt Kunden bereits heute mit mehreren aufeinander abgestimmten Dienstleistungsbausteinen, die exakt auf die kommenden Anforderungen ausgerichtet sind – auch wenn diese erst ab 2027 rechtlich greifen. Ein zentraler Baustein ist der Softwarewartungsvertrag, der über die reine Fehlerbehebung hinausgeht. Regelmäßige Sicherheitsupdates für Betriebssysteme, Datenbanken und Laufzeitumgebungen werden strukturiert geplant, getestet und in Abstimmung mit dem Kunden ausgerollt. Dabei sorgt ein vierteljährlicher Health Check für Transparenz bezüglich des Systemzustands, dokumentiert den Patchstatus und liefert proaktiv Hinweise auf mögliche Schwachstellen.

Die Ergebnisse werden in Form eines Berichts zur Verfügung gestellt und können im Sinne der Nachweispflichten gegenüber Behörden oder Auditoren verwendet werden.

Ein weiteres zukunftsorientiertes Angebot ist der Automation-Check-up. Dabei handelt es sich um eine vorausschauende Wartungsstrategie, die deutlich mehr leistet als eine technische Instandhaltung. In einem mehrstufigen Prozess analysiert Unitechnik systematisch Störmeldungen, bewertet den Softwarestand und empfiehlt konkrete Maßnahmen zur Optimierung und Risikoabsicherung. Besonders hervorzuheben sind die Integration sicherheitsrelevanter Softwareupdates und die strukturierte Nachverfolgung ihrer Wirksamkeit – ein Vorgehen, das in der neuen Maschinenverordnung ausdrücklich gefordert wird. Ein Beispiel für sicherheitsrelevante

Softwareupdates sind Antriebsregler. Hier wird regelmäßig geprüft, ob die Firmware des Herstellers auf dem neuesten Stand ist.

Darüber hinaus unterstützt Unitechnik aktiv bei der Migration veralteter Steuerungssysteme. Die Umstellung von Siemens Step7 auf das moderne TIA-Portal ist aus technischer Sicht längst überfällig und gewinnt durch die Sicherheitsanforderungen an Dringlichkeit. Denn ältere Engineering-PCs mit Windows XP oder 7, wie sie häufig für Step7 benötigt werden, bergen ein erhebliches Sicherheitsrisiko.

Die TIA-Plattform hingegen erlaubt nicht nur den Einsatz aktueller Hardware, sondern auch die Einbindung von sicheren Kommunikationsprotokollen, Benutzerrechteverwaltung und Diagnosefunktionen. All dies sind essenzielle Elemente moderner Cybersecurity-Konzepte.

Auch im Bereich der Systemarchitektur setzt Unitechnik auf Sicherheit: Der Zugang zu Kundensystemen erfolgt grundsätzlich über virtuelle Maschinen. In dieser virtuellen Umgebung, die exklusiv für einen Kunden genutzt wird, sind die individuellen Zugangsmechanismen sowie alle benötigten Entwicklungs- und Diagnosewerkzeuge installiert.

Im Falle eines Angriffs ist dadurch eine Isolation gewährleistet, die verhindert, dass Schadsoftware von einem Kundensystem auf ein anderes übertragen werden kann. Diese Maßnahme entspricht dem Prinzip der Segmentierung, wie es in vielen Sicherheitsstandards empfohlen wird.

## Das Fazit: Cybersecurity wird Pflicht, Anbieter liefern Lösungen

Die neuen EU-Regularien markieren den Beginn eines neuen Zeitalters in der industriellen Automatisierung. Cybersicherheit ist keine nette Zusatzoption mehr, sondern eine gesetzlich verankerte Pflicht. Betreiber und Inverkehrbringer sind gleichermaßen gefordert, über den gesamten Lebenszyklus ihrer Systeme hinweg für Schutz, Transparenz und Reaktionsfähigkeit zu sorgen.

Automatisierungsspezialisten wie Unitechnik nehmen sich dieser Herausforderung an – nicht erst ab 2027, sondern schon heute. Mit einem durchdachten Portfolio von Wartungs- und Migrationsdienstleistungen sowie einem tiefen Verständnis der regulatorischen Anforderungen unterstützen diese Fachfirmen die Kunden dabei, ihre Anlagen nicht nur effizient, sondern auch zukunftssicher zu betreiben. So wird Cybersecurity zum festen Bestandteil der Intralogistik – technisch, organisatorisch und rechtlich. *(jak)*

Eine Information von Unitechnik  
Firmenprofil siehe Seite 79

## In Überblick

### Unterschied zwischen IT-Security und OT-Security

**IT-Security** (Information Technology Security) schützt klassische Unternehmens-IT wie Server, Netzwerke und Daten vor Cyberangriffen, wobei Vertraulichkeit, Integrität und Verfügbarkeit im Fokus stehen.

**OT-Security** (Operational Technology Security) hingegen bezieht sich auf die Absicherung von industriellen Steuerungs- und Automatisierungssystemen, bei denen vor allem die Verfügbarkeit und die Sicherheit physischer Prozesse (z.B. Materialfluss) im Vordergrund stehen.



**Während IT-Security stärker softwaregetrieben ist, erfordert OT-Security ein tiefes Verständnis für Maschinen und Anlagen sowie deren Echtzeitverhalten.**

Mit PSiWms AI Effizienz der Auftragsabwicklung um mehr als 20% steigern



[www.psi.de](http://www.psi.de)

Software for Logistics Industry Leaders

PSI 

**TGW LOGISTICS**

Ludwig Szinicz Straße 3  
4614 Marchtrenk  
ÖSTERREICH

Telefon +43 50 486  
E-Mail systems@tgw-group.com  
Internet www.tgw-group.com

**Standorte** **Vertriebsstandort in Deutschland**  
TGW Systems Integration GmbH  
Robert-Bosch-Straße 11a  
63225 Langen bei Frankfurt  
Tel.: +49 6103 924-7610

**Geschäftsführung** Thomas Berndorfer  
Martin Waldenberger  
Klaus Prechtl

**Gründungsjahr** 1969

**Beschäftigte** 4.500

**Jahresumsatz** 1,07 Mrd. EUR (FY 2023/24)

**Produkt- und Dienstleistungsprogramm**

TGW Logistics ist ein weltweit führender Systemanbieter von automatisierten, schlüsselfertigen Logistikkösungen sowie selbstlernender Robotik.

Seit 1969 realisieren wir Logistikkösungen für Unternehmen in Fashion, Lebensmittelhandel und Industrie- und Konsumgüter.

Der Hauptsitz befindet sich in Marchtrenk in Oberösterreich. Vertrieb und Service-niederlassungen sowie ein umfangreiches Distributorennetzwerk bedienen Kunden weltweit in über 45 Ländern – von Europa, über Nordamerika, APAC und Südamerika bis Australien. Die Produktionsstandorte von TGW Logistics befinden sich in Europa und China.

**Kernkompetenzen**

- Systemintegration
- Systemanalyse und -planung
- Optimierung/Modernisierung
- Projektmanagement

**Referenzen im Bereich Modernisierung / Maintenance**

- Aesculap
- Almi
- GAP
- Kärcher
- Musikhaus Thomann
- Esprit
- Wilhelm Fricke Landmaschinen

**Ihr Ansprechpartner Modernisierung / Maintenance**

Markus Kammerhofer  
Director Sales Retro  
Tel.: +43 50 486-3799



**Unitechnik Systems GmbH**

Fritz-Kotz-Straße 14  
51674 Wiehl

Telefon +49 2261 987-0  
E-Mail logistics@unitechnik.com  
Internet www.unitechnik.com

**Geschäftsführung** Torsten Ley

**Gründungsjahr** 1971

**Beschäftigte** 202 (314 in der Unitechnik Group)

**Jahresumsatz** 53,3 Mio. EUR

**Produkt- und Dienstleistungsprogramm**

**Planung und Realisierung von passgenauen Gesamtanlagen für die innerbetriebliche Logistik:**

- Automatisierte Logistikzentren
- Produktionslogistik
- Lagerverwaltungssoftware UniWare
- Anlagenmodernisierung

**Kernkompetenzen**

- Logistik Consulting
- Generalunternehmer und Systemintegrator
- Softwareentwicklung (LVS, MFR und SPS)
- Elektrokonstruktion und Schaltanlagenbau
- Montage, Inbetriebnahme und Schulung
- Wartung und Service (24/7) für Gesamtanlage
- Retrofit im laufenden Betrieb

**Referenzen im Bereich Modernisierung / Maintenance**

A.S.Création, apt Hiller, B.Braun, Benteler, C.D. Wälzholz, DEHN, Deutsche Bahn, Eaton Electric, Georg Fischer, Hela, INL (Dubai), Jokey, Kostal, Meyer Werft, Radium, Scheidt&Bachmann, soft-carrier, Soennecken, Turck, VOSS, ...

**Ihr Ansprechpartner Modernisierung / Maintenance**

Christian Mertens  
Tel.: +49 2261 987-502  
E-Mail: christian.mertens@unitechnik.com

