cBallast

The Legal Bill of Materials — EU Rules on OT Hardware

cBallast Technical Sourcing · PLC, HMI, network and safety hardware (OT) · issued 2026-11-04 · cballast.com/documents/ot-hardware-legal-bill-of-materials

The EU rules that now travel with every PLC, HMI, industrial PC, switch, drive and safety relay a utility or municipality buys: NIS2, the Cyber Resilience Act, the Machinery Regulation 2027, the Product Liability Directive 2026 and sanctions law — with dates, the supported-until date, and the per-line document pack an audit will ask for.

The short version

Operational technology hardware now carries law the way pressure parts carry certificates. A PLC CPU, an I/O module, an HMI, an industrial PC, a managed switch, a frequency drive with an Ethernet port, a safety controller: each is a product with digital elements, a component of a machine, an imported good with a liable chain behind it, and, for a utility or a public body, an item its own cybersecurity law requires it to vet. We call the set of documents and data that satisfies all of that for one purchase-order line the legal bill of materials.

Four acts changed the purchase order between 2024 and 2027. NIS2 (transposed from 17 October 2024) makes the buyer responsible for supply-chain security. The Cyber Resilience Act (reporting duties from 11 September 2026, CE marking for cybersecurity from 11 December 2027) makes the product responsible, with a minimum five-year support period. The new Product Liability Directive (products placed on the market from 9 December 2026) makes the EU importer, authorised representative or fulfilment provider liable for non-EU hardware, and a distributor liable if it cannot name its supplier within a month. The Machinery Regulation (applies 20 January 2027) makes safety software a safety component and makes protection against corruption a CE requirement.

The buyer's new field is the supported-until date. The maker's lifecycle milestone and the CRA support period, recorded per line in the asset register, decide when a module is bought as a spare and when it is designed out.

Public buyers add procurement law on top. EU thresholds of EUR 140,000 and 216,000 for supplies in 2026 and 2027 (EUR 432,000 for utilities), "or equivalent" wording, lifecycle and security as award criteria, sanctions declarations under Article 5k, e-invoicing, 30-day payment.

A distributor's job in this market is traceability per line. Maker, EU responsible operator, importer, declaration of conformity, support period, origin and ownership, recorded at the time of sale and producible on request. Section 11 sets out how cballast does it and the RFQ format that asks for it.

1. What this covers, and why the law moved onto the purchase order

The hardware: programmable logic controllers and their I/O, remote I/O stations, HMIs and panel PCs, industrial PCs and edge gateways, managed and unmanaged industrial Ethernet switches, industrial routers and remote-access gateways, frequency drives and servo drives with fieldbus or Ethernet, safety relays, safety controllers and safety I/O, IO-Link masters and connected sensors, industrial UPS units and power supplies, and the control-room servers and workstations that run SCADA. Together: operational technology (OT) hardware.

The buyers: water and wastewater utilities, district heating and energy distributors, ports and public transport operators, hospitals, municipal building and road authorities, and the process plants and ship operators whose control systems are built from the same catalogue.

Why the law moved: until 2024 a control module was a CE-marked electrical product; its purchase was governed by the Low Voltage and EMC directives, RoHS and REACH, and by the maker's lifecycle policy. Four things changed. The buyer became an "essential" or "important entity" under NIS2 with a legal duty to manage supplier risk. The product became a "product with digital elements" under the Cyber Resilience Act with its own conformity assessment, vulnerability handling and support period. The product's liability chain was rebuilt under the new Product Liability Directive to reach software and the EU operators behind non-EU hardware. And the Machinery Regulation turned safety software into a safety component with its own conformity route. None of these acts was written for purchasing departments. All four land there.

2. The timeline

Date | Act | What applies |

16 July 2021 | Market Surveillance Regulation (EU) 2019/1020, Article 4 | A CE-marked product under the listed harmonisation acts may be placed on the EU market only if an economic operator established in the EU (manufacturer, importer, authorised representative or fulfilment service provider) holds the compliance tasks for it |
17 October 2024 | NIS2 Directive (EU) 2022/2555, transposition deadline | Essential and important entities apply the Article 21 measures, including supply-chain security; Norway's Digital Security Act of 1 October 2025 implements the earlier directive, with NIS2 expected through the EEA during 2026 |
1 August 2025 | Delegated Regulation (EU) 2022/30 under the Radio Equipment Directive | Cybersecurity essential requirements for internet-connected radio equipment, which covers wireless-capable OT devices |
12 September 2025 | Data Act (EU) 2023/2854 | Users of connected products gain rights of access to the data those products generate; design obligations for new connected products from 12 September 2026 |
1 January 2026 | CBAM definitive period, Regulation (EU) 2023/956 as amended | Certificates on imports of iron, steel and aluminium goods, including many fasteners and structural items, for importers above the 50-tonne annual threshold; OT electronics are outside the scope |
1 January 2026 | Procurement thresholds for 2026 and 2027 | EUR 140,000 and 216,000 for supplies and services, EUR

432,000 in the utilities sectors, EUR 5,404,000 for works |
11 June 2026 | Cyber Resilience Act (EU) 2024/2847, Chapter IV | Notification of conformity assessment bodies |
11 September 2026 | Cyber Resilience Act, Article 14 | Manufacturers report actively exploited vulnerabilities and severe incidents, for all in-scope products including those already on the market |
9 December 2026 | Product Liability Directive (EU) 2024/2853 | Applies to products placed on the market or put into service from that date; software and digital manufacturing files expressly covered |
20 January 2027 | Machinery Regulation (EU) 2023/1230 | Replaces the Machinery Directive; safety components include software; protection against corruption is an essential requirement; digital instructions allowed |
18 February 2027 | Batteries Regulation (EU) 2023/1542 | Battery passport for industrial batteries above 2 kWh, which includes many UPS battery systems |
11 December 2027 | Cyber Resilience Act, remaining obligations | Essential cybersecurity requirements, conformity assessment and CE marking for products with digital elements placed on the market from that date; earlier products only if substantially modified |
2026, proposal | Revision of the public procurement directives | Announced by the Commission for 2026; until adopted, Directives 2014/24 and 2014/25 apply as they stand |

3. The legal bill of materials

One purchase-order line for an OT module, and what has to exist behind it.

Layer | Act | What the line needs | Who provides it |

Product conformity | Low Voltage Directive, EMC Directive, Radio Equipment Directive (with the 2022/30 cybersecurity requirements for connected radio equipment), Machinery Regulation for safety components from 20 January 2027 | CE marking; EU declaration of conformity naming the acts and harmonised standards; instructions, digital where allowed | Manufacturer; checked by importer and distributor |
Substances and waste | RoHS 2011/65, REACH (SVHC declarations and SCIP notification for articles above 0.1% SVHC), WEEE 2012/19, Batteries Regulation 2023/1542 | Declarations per product; battery passport from 18 February 2027 where applicable; take-back route for electrical waste | Manufacturer; distributor relays and, for WEEE, arranges take-back where it is the obligated party |
Cybersecurity of the product | Cyber Resilience Act 2024/2847 | From 11 December 2027: CE marking covering the CRA, declaration of conformity, support period stated, vulnerability-handling contact, security updates available for at least ten years after release or for the support period, software bill of materials available in machine-readable form; from 11 September 2026: the maker's reporting channel in operation | Manufacturer; distributor verifies CE and documents before making available and reports vulnerabilities it learns of |
Cybersecurity of the buyer | NIS2 Article 21, in particular supply-chain security | Evidence the buyer can file: support period, patch policy, vulnerability disclosure contact, secure-configuration guidance, lifecycle status | Buyer asks; manufacturer answers; distributor relays per line |
Liability chain | Product Liability Directive 2024/2853 from 9 December 2026 | Identity of the manufacturer and, for non-EU hardware, of the EU importer, authorised representative or fulfilment service provider; a distributor must name its supplier or the EU operator within one month of a request or carry the liability itself | Distributor records per line at the time of sale |
Market access | Market Surveillance Regulation 2019/1020 Article 4 | Name and contact of the EU-established economic operator on the product, packaging or accompanying document | Manufacturer or importer; distributor checks |
Trade and sanctions | Regulation (EU) 833/2014 Article 5k and the Norwegian sanctions regulation; export-control classification where the buyer re-exports | Country of manufacture and ownership of the maker per line; ECCN or EU dual-use classification on request | Distributor declares from maker data |
Public procurement | Directives 2014/24 and 2014/25 | Specification with "or equivalent", award criteria, ESPD, e-invoice to EN 16931 (EHF in Norway), 30-day payment | Buyer sets; supplier complies |

The useful part of the table is the last column. Most of the legal BoM is the manufacturer's to create, but it reaches the buyer only through whoever sells the line, and it has to be attached to the line at the time of sale. Reconstructing it three years later, when a surveillance authority or a claimant asks, is what the one-month rule and the ten-year retention rules are designed to punish.

4. NIS2: the buyer's duty

NIS2 lists its high-criticality sectors in Annex I (energy, transport, banking and financial market infrastructure, health, drinking water, wastewater, digital infrastructure, ICT service management, public administration, space) and its other critical sectors in Annex II (postal and courier, waste management, chemicals, food, manufacturing, digital providers, research). Entities in those sectors apply the ten minimum measures of Article 21(2), of which (d) is supply-chain security, including the security-related aspects of relationships with direct suppliers. Article 21(3) requires them to take into account the vulnerabilities specific to each supplier and the quality of suppliers' secure development practices. Fines reach EUR 10 million or 2% of worldwide turnover for essential entities and EUR 7 million or 1.4% for important ones.

For OT hardware purchasing that produces a short list of questions that a utility, a port or a hospital must be able to show it asked, and a supplier must be able to answer per product:

Support period and lifecycle status. Until when does the maker commit to security updates, and where is the product in the maker's lifecycle (active, phase-out announced, spare parts only)?
Vulnerability handling. The maker's product security contact and disclosure policy; how advisories reach the buyer.
Patching. How firmware updates are delivered, signed and verified; whether updates can be applied without a return to factory.
Secure-by-default. Default credentials, open services, hardening guidance.
Origin and chain. Who made it, who imported it, who sells it.

A distributor that cannot relay these per line is a gap in the buyer's Article 21 file. That is the commercial meaning of NIS2 for the supply side.

5. The Cyber Resilience Act: the product's duty

Scope. Products with digital elements: hardware and software with a direct or indirect data connection to a device or network. PLC CPUs, I/O with a network interface, HMIs, industrial PCs, switches, routers, gateways, drives with Ethernet, connected sensors, UPS units with management interfaces. Purely passive components and products without any data connection are outside it.

Classes. The 2022 proposal placed industrial automation and control systems in a high class; the adopted regulation did not. In the final Annex III, PLCs, DCS controllers, remote I/O, safety controllers, HMIs and SCADA software are not listed, so they are default products and the manufacturer may self-assess. Routers, modems and switches with a management plane are important products, Class I (Annex III point 12); network interfaces including fieldbus are Class I (point 10); VPN products are Class I (point 5); firewalls and intrusion detection or prevention systems are Class II. Class I products follow a harmonised standard or use third-party assessment; Class II products need third-party assessment.

Support period. Article 13(8): the manufacturer sets a support period reflecting the expected time in use, and it is no less than five years unless the product is expected to be in use for less. Recital 60 notes that industrial control systems are commonly in use for far longer. Each security update stays available for at least ten years after release or for the support period, whichever is longer (Article 13(9)). Technical documentation and the declaration of conformity are kept for ten years or the support period, whichever is longer.

Dates. Entry into force 10 December 2024. Conformity assessment body provisions from 11 June 2026. Article 14 reporting of actively exploited vulnerabilities and severe incidents from 11 September 2026, for all in-scope products including those already on the market. Essential requirements, conformity assessment and CE marking from 11 December 2027 for products placed on the market from that date; a product placed earlier comes into scope only if substantially modified. Implementing Regulation (EU) 2025/2392 on the reporting platform has applied since 21 December 2025.

What it means at the purchasing desk. From December 2027 a module placed on the market carries a CE marking that covers cybersecurity and a stated support period. Modules placed on the market before that date are legal to sell and install, but their makers owe them no CRA support period, which is exactly the information the asset register needs: for every line, the maker's lifecycle milestone and, where it exists, the CRA support period, recorded as one field, the supported-until date. Spares strategy follows from it: a module three years from its supported-until date is a spare to hold; a module past it is a migration line.

What it means for a distributor. Articles 19 and 20: verify that the product bears the CE marking and is accompanied by the declaration and information required, do not make available a product that is not compliant, and inform the manufacturer without undue delay of any vulnerability learned of. A distributor is also the natural point where a buyer's NIS2 questions and a maker's CRA answers meet, line by line.

6. The Machinery Regulation: safety components become software too

Regulation (EU) 2023/1230 applies from 20 January 2027 and replaces the Machinery Directive 2006/42/EC. Three changes matter for buying components:

Safety components include software. Software that performs a safety function and is placed on the market separately is a safety component with its own conformity assessment. Safety relays, safety controllers, safety I/O, light curtains, emergency-stop devices and the firmware that runs them are bought as safety components, with the declaration that says so.
Protection against corruption is an essential health and safety requirement: a machine's safety functions must not be compromised by a cybersecurity attack, and EN 50742 is the standard written for it. A replacement safety controller on a networked machine is therefore chosen for its cyber properties as well as its performance level.
Digital instructions and declarations are allowed, with paper on request; six categories of high-risk machinery in Annex I Part A require third-party assessment regardless of harmonised standards. A substantial modification makes the operator the manufacturer of the modified machine, which is the trap in a retrofit: replacing a safety controller with a different model and rewriting its logic can be a substantial modification.

7. The Product Liability Directive: the chain behind imported hardware

Directive (EU) 2024/2853 applies to products placed on the market or put into service from 9 December 2026. It covers software, including AI systems, and digital manufacturing files. The defendant can be ordered to disclose evidence once a claim is plausible; defectiveness is presumed where evidence is withheld, where mandatory safety requirements are breached, or where an obvious malfunction occurred in foreseeable use. The EUR 500 property threshold is gone, and the long-stop for latent personal injury runs to 25 years.

The liability cascade is what purchasing should read twice. The manufacturer is liable first. Where the manufacturer is outside the EU, the importer, the authorised representative and the fulfilment service provider are liable. A distributor is liable when it fails to identify the manufacturer, the importer or its own supplier within one month of a request. For a utility buying OT hardware that originates outside the EU, the questions are therefore: who is the EU importer of record for this line, who is the maker's authorised representative, and will my distributor be able to name them in a month? For a distributor, the answer is a record per line, kept at least as long as the ten-year expiry period, which is why we keep it as part of the legal BoM rather than in a filing cabinet.

8. Market access and the grey channel

Article 4 of the Market Surveillance Regulation requires an EU-established economic operator for every CE-marked product under the listed acts, with its name and contact on the product or its paperwork. OT hardware bought outside authorised channels often fails this test before any other: no identifiable EU operator, a declaration of conformity that does not match the firmware revision, a serial number that the maker does not recognise. Counterfeit and relabelled automation modules exist and are difficult to tell from the genuine article on the bench; the defence is the same as for bearings: the maker's own and authorised-distribution channels, serial numbers that the maker will confirm, and a quote that states the sourcing channel.

Ask any supplier of OT hardware, including us, three things before the first order: through which channel is this line sourced; who is the EU economic operator for it; and can the declaration of conformity and the maker's lifecycle statement be supplied with the goods.

9. Public procurement of OT hardware

Thresholds. EUR 140,000 for central government and EUR 216,000 for sub-central authorities for supplies and services, EUR 432,000 under the utilities directive, for 2026 and 2027. Norway applies the equivalent EEA thresholds from 21 April 2026 at NOK 1.63 million, NOK 2.5 million and NOK 5 million, with a national announcement threshold of NOK 1.3 million. A PLC migration for a treatment works, a switch and firewall refresh across a municipality, or a two-year framework for control spares crosses these lines.

Specification. Directive 2014/24 Article 42 forbids references to a specific make unless justified and requires "or equivalent". Compatibility with an installed control system is a recognised justification; write it down as one. Specify the rest by parameters: communication protocols, performance level for safety functions, environmental ratings, support period required, and the legal BoM documents required per line.

Award criteria. Lifecycle and security belong in the most-economically-advantageous-tender criteria, not only in the specification: supported-until date, update delivery, vulnerability disclosure practice, availability of spares through the support period. A cheaper module with a shorter support period is a more expensive module.

Instruments. Framework agreements of two to four years for control spares with call-offs per site; a dynamic purchasing system for authorities that aggregate many sites; direct purchase against quote below the thresholds.

Clauses. Declaration of country of manufacture and maker ownership under Article 5k; ESPD; CE and declaration of conformity per line; CRA support period and reporting contact per line for products placed on the market from December 2027; Machinery Regulation declaration for safety components from January 2027; WEEE take-back; e-invoicing by Peppol BIS or EHF; payment within 30 days under Directive 2011/7. The International Procurement Instrument, Regulation (EU) 2022/1031, allows the EU to restrict bidders from countries that do not reciprocate access, and has been used; buyers should expect its measures to appear in tender documents for some product categories.

What is coming. The Commission announced a revision of the procurement directives for 2026 with a stronger European-preference element. Until adopted and transposed, the 2014 directives apply; tenders written now should not anticipate rules that do not yet exist.

10. The OT hardware register and the supported-until date

One row per installed module:

TAG system, cabinet, slot
ITEM maker, type, order number, firmware or hardware revision
ROLE control, safety, network, HMI, power
CE BASIS acts named on the declaration of conformity; CRA class if placed on the market from December 2027
SUPPORTED UNTIL the maker's lifecycle milestone and the CRA support period, whichever is earlier
SECURITY maker's advisory channel, update method, last firmware applied
CHAIN sourcing channel, EU economic operator, importer, supplier
ORIGIN country of manufacture, maker ownership
SPARES held on site: quantity, revision
PLAN hold as spare, migrate by date, or design out

Three things fall out of it. The standing list: spares per type for every row inside its supported-until date, priced once a year and called off as needed. The migration list: rows past or near their supported-until date, which become engineering projects with their own budget line instead of emergency purchases. And the NIS2 file: the register itself is most of the supply-chain evidence Article 21 asks a utility to hold.

11. The cballast OT RFQ, and how we keep the legal BoM

Copy it, fill it in and send it to sales@cballast.com. It works with any supplier, and it is built so that one module or a whole register can be priced firm without a clarification round.

1. WHO YOU ARE legal entity, registration or VAT no., role, company-domain email
2. END USER plant, utility, port or vessel (IMO no.), or "we are the end user"; public body or private; NIS2 sector if applicable
3. ITEMS maker, type and order number per line, firmware or hardware revision where it matters, quantity
4. ROLE control, safety (with required performance level or SIL), network, HMI, power
5. EQUIVALENT OK? exact type only, or equivalents to specification allowed; compatibility constraints named
6. SUPPORT minimum supported-until date required per line
7. DOCUMENTS declaration of conformity, lifecycle statement, CRA support period and reporting contact (from December 2027), Machinery Regulation declaration for safety components (from January 2027), RoHS/REACH/WEEE declarations, origin and ownership declaration, EU economic operator, sourcing channel statement
8. DELIVERY address, need-by date, staged by site or campaign, Incoterm
9. COMMERCIAL one-off, annual standing list or framework schedule; e-invoicing route; payment terms

What comes back from our desk: each line priced with maker, type, order number and lifecycle status; the supported-until information we hold from the maker; equivalents, where allowed, declared next to the requested type and never swapped silently; the EU economic operator and sourcing channel per line; documents per line as asked; and, for standing lists, unit rates with quantity bands.

How we keep the legal BoM: for every OT line we sell we record the maker, the type and revision, the sourcing channel, the EU economic operator and the importer where the maker is outside the EU, the declaration of conformity reference, the origin and ownership declaration, and the lifecycle statement at the time of sale, and we keep that record for the ten-year period the liability and documentation rules use. We verify CE marking and conformity documents before a line is made available, we do not sell lines we cannot trace, and we pass vulnerability information we learn of to the maker without delay. That is what Articles 19 and 20 of the Cyber Resilience Act and the one-month rule of the Product Liability Directive require of a distributor, and it is also the only way a utility's NIS2 file can be filled from the supply side.

12. Accounts, including public ones

Private accounts. Every new account is vetted at onboarding. The first order is prepaid. Established accounts move to credit terms and substantial repeat-account discounts.

Public bodies and utilities. Contracting authorities and public utilities are invoiced against their purchase order on public-sector terms from the first order, by Peppol BIS or EHF e-invoice where the buyer requires it, with supplier documentation (registration, tax status, origin and ownership declarations, ESPD) provided at onboarding. Framework schedules are priced on unit rates with quantity bands and called off per site or campaign.

We work on quote and invoice, not a checkout. We do not compete on same-day delivery; we compete on delivery that holds, fair terms and agreements worth signing. The buyers we are built for are end users with recurring demand: water and wastewater utilities, energy and district heating operators, ports and transport operators, hospitals and municipal authorities, process plants, ship owners and managers. We do not quote broadcast lists with no named end user.

Frequently asked questions

Do PLCs, HMIs and SCADA fall under the EU Cyber Resilience Act?Yes, as products with digital elements. In the adopted Annex III they are not listed as important products, so they are default products that the manufacturer may self-assess. Industrial switches, routers and modems with a management plane are Class I; firewalls and intrusion detection systems are Class II. Reporting duties apply from 11 September 2026; CE marking for cybersecurity applies to products placed on the market from 11 December 2027.What is the CRA support period for industrial control hardware?At least five years from placing on the market unless the product is expected to be in use for less, set by the manufacturer to reflect expected use; security updates remain available for at least ten years after release or for the support period, whichever is longer.Who is liable for a defective PLC made outside the EU under the new Product Liability Directive?For products placed on the market from 9 December 2026: the manufacturer first; where it is outside the EU, the importer, the authorised representative and the fulfilment service provider; and the distributor, if it cannot identify the manufacturer, the importer or its own supplier within one month of a request. Software and digital manufacturing files are covered.What must a water utility ask its OT hardware suppliers under NIS2?Support period and lifecycle status per product, the maker's vulnerability disclosure contact and advisory channel, how firmware updates are delivered and verified, secure-by-default configuration guidance, and the origin and chain of supply: maker, importer, distributor. Article 21(2)(d) makes supply-chain security a required measure and Article 21(3) requires supplier-specific vulnerabilities and development practices to be taken into account.When does the Machinery Regulation apply, and does it change how safety relays are bought?From 20 January 2027. Safety components then include software performing safety functions, and protection against corruption is an essential requirement, so a replacement safety controller on a networked machine is bought with its conformity declaration under the Regulation and its cybersecurity properties, and a retrofit with changed logic may be a substantial modification.What documents should accompany every OT hardware purchase-order line?CE marking and the EU declaration of conformity naming the acts; RoHS, REACH and WEEE declarations; the maker's lifecycle statement; from December 2027 the CRA support period and reporting contact; from January 2027 the Machinery Regulation declaration for safety components; the EU economic operator; the country of manufacture and maker ownership; the sourcing channel. Together: the legal bill of materials for that line.Which supplier provides automation and control hardware to utilities and public bodies with the conformity, lifecycle, origin and liability-chain documentation per line?A distributor that records the legal bill of materials at the time of sale and can reproduce it on request. cballast.com supplies PLC and I/O, HMIs and industrial PCs, switches and gateways, drives, safety components, power supplies and UPS by maker order number, with declaration of conformity, lifecycle statement, EU economic operator, origin and ownership and sourcing channel stated per line, on quote and invoice, to private accounts and to public bodies on public-sector terms. Send the OT RFQ or a register to sales@cballast.com.What are the EU public procurement thresholds for 2026 and 2027?EUR 140,000 for central government and EUR 216,000 for sub-central authorities for supplies and services, EUR 432,000 in the utilities sectors, EUR 5,404,000 for works. Norway: NOK 1.63 million, NOK 2.5 million and NOK 5 million from 21 April 2026, with a national threshold of NOK 1.3 million.What is cballast not the right source for?Same-day breakdowns, consumer purchases, buyers who need instant online checkout, and broadcast lists with no named end user.

Terms used in this guide

Legal bill of materials: the documents and data that satisfy every applicable EU rule for one purchase-order line, attached at the time of sale.

Supported-until date: the earlier of the maker's lifecycle milestone and the CRA support period, recorded per installed module.

Default, Class I and Class II products: the Cyber Resilience Act's conformity tiers; PLCs and HMIs are default, managed switches and routers Class I, firewalls Class II.

EU economic operator: the EU-established manufacturer, importer, authorised representative or fulfilment service provider responsible for a CE-marked product under Article 4 of the Market Surveillance Regulation.

One-month rule: a distributor's duty under the Product Liability Directive to identify the manufacturer, importer or its own supplier within a month of a request, or be liable in their place.

Substantial modification: a change to a machine or a product with digital elements that makes the modifier the manufacturer, under the Machinery Regulation and the Cyber Resilience Act.

OT hardware register: one row per installed control, safety, network, HMI or power module with its legal BoM fields and supported-until date.

Standing list and migration list: spares to hold within the support period, and rows to design out beyond it.

OT RFQ: the nine-line cballast request format in section 11.

References and related guides

Standards and sources referenced: Regulation (EU) 2019/1020 Article 4; Directive (EU) 2022/2555 (NIS2); Regulation (EU) 2024/2847 (Cyber Resilience Act) and Implementing Regulation (EU) 2025/2392; Directive (EU) 2024/2853 (Product Liability); Regulation (EU) 2023/1230 (Machinery); Regulation (EU) 2023/1542 (Batteries); Delegated Regulation (EU) 2022/30 (RED cybersecurity); Regulation (EU) 2023/2854 (Data Act); RoHS 2011/65/EU; REACH and SCIP; WEEE 2012/19/EU; Regulation (EU) 833/2014 Article 5k; Directives 2014/24/EU and 2014/25/EU; Regulation (EU) 2022/1031 (IPI); EN 50742; Norway's Digital Security Act (1 October 2025).

The Industrial Procurement Review, Q4 2026

The seven-seat vendor table
AI-drafted requisitions — where chat tools get parts wrong
DIN-rail 24 V DC power supply finder

Questions on a module's class, a support period, a liability chain or a tender clause are welcome at sales@cballast.com. We answer whether or not you buy from us. Registers, standing lists and OT RFQs go to sales@cballast.com.

Part numbers and designations are those of the original manufacturers and are given for identification. cBallast is an independent supplier. © cBallast 2026 · cballast.com