OT security checklist for cranes and yard equipment

For: Maintenance, automation and electrical engineers of a container or multipurpose terminal

Walk the checklist with the people who maintain the cranes and the yard equipment, one machine class at a time (ship-to-shore cranes, yard cranes, straddle and shuttle carriers, other yard equipment). For each line, write who owns it, where the evidence is kept and its status. A line that cannot be checked without stopping a machine is planned for the next maintenance window, never tested on a working crane.

Scope. Operational technology (OT) means the programmable systems that monitor or control physical equipment (NIST SP 800-82 Rev. 3). On a terminal this covers the crane and equipment controls, their networks and radios, the systems that link them to the terminal operating system (TOS), and the remote access used by the equipment suppliers. The office network (IT) and the TOS itself are covered by other pages of this site.

Machines covered

• **Ship-to-shore (STS) cranes**: Drive and control PLCs, safety controllers, cabin and e-house HMIs, crane management and condition monitoring, cameras, the link to the TOS.

• **Yard cranes (RTG, RMG, automated stacking cranes)**: The same layers, plus the radio or fibre link that follows the crane along the block and, for automated cranes, the remote operator stations.

• **Straddle and shuttle carriers**: On-board controllers and terminals, positioning, and the wireless network that carries job orders from the TOS.

• **Other yard equipment**: Reach stackers, terminal tractors and similar machines with an on-board terminal, telematics or a supplier's remote monitoring.

Status

• in place · the evidence exists, is dated and someone owns it

• partial · done for some machines or some links only, or the evidence is out of date

• missing · nothing yet

• not applicable · write down why

Summary sheet · terminal: _____ · machine class: _____ · date: _____

Item	References	Status	Owner
A1 · One inventory for every machine	NIST SP 800-82r3 6.1.1 · IMO Rev.4 3.5.2.2		
A2 · Software and firmware versions recorded	NIST SP 800-82r3 6.1.1		
A3 · Every connection drawn	IMO Rev.4 3.5.2.2 · NIST SP 800-82r3 5.2.3.1		
A4 · The inventory is updated after each maintenance	NIST SP 800-82r3 6.1.1		
A5 · Discovery tools tested before they touch a crane	NIST SP 800-82r3 6.1.1		
Z1 · Equipment grouped into zones	NIST SP 800-82r3 5.2.3.1 · ISA/IEC 62443 (zones and conduits)		
Z2 · Only documented flows cross a zone boundary	NIST SP 800-82r3 5.2.3.1		
Z3 · OT apart from IT and from the Internet	IMO Rev.4 3.5.3.3 · 33 CFR 101.650(e) and (h)		
Z4 · Yard radio networks treated as a separate segment	NIST SP 800-82r3 6.2.9		
Z5 · Electrical rooms, cabins and ports physically closed	33 CFR 101.650(i)		
R1 · Every remote access path is known	USCG notices, 23 Feb 2024 and 19 Nov 2024 · IMO Rev.4 3.5.3.8		
R2 · Remote access requested, justified and limited	NIST SP 800-82r3 6.2.10		
R3 · Named accounts and multi-factor authentication	NIST SP 800-82r3 6.2.10 · IMO Rev.4 3.5.3.1-3.5.3.2		
R4 · Remote access never bypasses safety or security controls	NIST SP 800-82r3 6.2.10		
R5 · The contract says how the supplier connects	IMO Rev.4 3.5.3.8 · NIST SP 800-82r3 4.2.1, 6.1.5		
P1 · A written OT patch process	NIST SP 800-82r3 6.2.11		
P2 · Patches tested before they reach a working machine	NIST SP 800-82r3 6.2.11		
P3 · Unsupported systems have compensating controls	NIST SP 800-82r3 6.2.11		
P4 · Maintenance laptops and media controlled	NIST SP 800-82r3 6.2.5, 6.2.7 · IMO Rev.4 3.5.3.5		
P5 · Configuration checked after maintenance	NIST SP 800-82r3 6.2.5		
S1 · Safety functions work without the network	NIST SP 800-82r3 2.3.7, 4.2.2		
S2 · A known safe state on loss of communication	NIST SP 800-82r3 5.3.1		
S3 · Physical separation where safety requires it	NIST SP 800-82r3 5.3.1		
S4 · Cyber and safety assessments talk to each other	NIST SP 800-82r3 4.2.2		
D1 · IT-OT connections logged and watched	33 CFR 101.650(h) · IMO Rev.4 3.5.4		
D2 · Programs and configurations backed up and restorable	NIST SP 800-82r3 3.3.9 · IMO Rev.4 3.5.3.7		
D3 · Running and restarting without the network	NIST SP 800-82r3 3.3.9		

A · Asset inventory

Know every controller, HMI, switch, radio and remote link on every machine, with its software and firmware version.

A1 · One inventory for every machine *(NIST SP 800-82r3 6.1.1 · IMO Rev.4 3.5.2.2)*

What to check: Each crane and yard machine has a list of its programmable components: PLCs and safety controllers, drives, HMIs, industrial PCs, network switches, radios, cameras and remote access gateways, with make, model, location on the machine and owner.

Why: NIST SP 800-82 Rev. 3 calls a complete and accurate asset inventory critical for managing OT risk: it supports risk assessment, vulnerability management and obsolescence tracking (6.1.1). IMO Rev.4 asks for an inventory of digital systems and of their network connections (3.5.2.2).

Evidence to hold: [ ] The inventory per machine class, with the date of the last update · [ ] The owner of each machine class (maintenance, automation or a supplier under contract)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

A2 · Software and firmware versions recorded *(NIST SP 800-82r3 6.1.1)*

What to check: For each component, the inventory records the software and firmware versions installed, and the PLC program version currently running on the machine.

Why: NIST lists software and firmware inventory, with version numbers and a software bill of materials (SBOM) where available, among the elements of OT asset management (6.1.1). Without versions, no advisory can be matched to a machine.

Evidence to hold: [ ] Versions per component, as read on the machine, with the date read · [ ] The SBOMs received from suppliers, where they exist

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

A3 · Every connection drawn *(IMO Rev.4 3.5.2.2 · NIST SP 800-82r3 5.2.3.1)*

What to check: A diagram shows how each machine class is connected: to the TOS or crane management system, to the cameras and OCR, to the radio or fibre network of the yard, and to any supplier's remote access, with the direction of each data flow.

Why: IMO Rev.4 asks to identify internal and external system dependencies and network connections (3.5.2.2). NIST uses the mapped data flows to decide which communications the network should allow (5.2.3.1).

Evidence to hold: [ ] The network and data-flow diagram per machine class, dated · [ ] The list of external connections, with purpose and owner

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

A4 · The inventory is updated after each maintenance *(NIST SP 800-82r3 6.1.1)*

What to check: A component swapped, a firmware updated or a program changed during maintenance is written into the inventory the same week.

Why: NIST recommends updating inventory information when components are added, removed or changed (patched, new firmware, a component swapped during maintenance) (6.1.1).

Evidence to hold: [ ] The maintenance work orders that changed OT components, linked to the inventory updates

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

A5 · Discovery tools tested before they touch a crane *(NIST SP 800-82r3 6.1.1)*

What to check: Any automated discovery or scanning tool is first tried on an offline component or a test bench, and passive methods are preferred on working machines. Where no tool fits, the inventory is kept by hand.

Why: NIST warns that active scanning may have a negative impact on OT systems and recommends testing automated asset management tools on offline systems or components before using them in production (6.1.1).

Evidence to hold: [ ] The record of the bench or offline test of the tool · [ ] The rule that says which methods are allowed on working machines

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

Z · Zones and conduits

Group the equipment into zones, allow only the documented flows between them, keep OT apart from IT and from the Internet.

Z1 · Equipment grouped into zones *(NIST SP 800-82r3 5.2.3.1 · ISA/IEC 62443 (zones and conduits))*

What to check: The OT is divided into zones that make sense for the terminal: for example one zone per crane or per machine class, a zone for the crane management and remote monitoring servers, a zone for the supplier access, and the safety functions kept in their own layer.

Why: NIST describes grouping components into levels, tiers or zones as the step that comes before placing isolation devices between them (5.2.3.1). The ISA/IEC 62443 series uses the same idea of zones and conduits.

Evidence to hold: [ ] The zone model, with the components of each zone · [ ] The reason for each boundary (criticality, owner, location, supplier)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

Z2 · Only documented flows cross a zone boundary *(NIST SP 800-82r3 5.2.3.1)*

What to check: Each connection between two zones (a conduit) goes through a firewall or a one-way gateway whose rules allow only the flows of the diagram (A3). Outbound rules from the OT are as strict as inbound rules. The rules are reviewed at a set interval.

Why: NIST recommends rulesets that only permit connections between adjacent levels, tiers or zones, and outbound rules as stringent as inbound rules; a unidirectional gateway (data diode) is an alternative where data only needs to leave the OT (5.2.3.1).

Evidence to hold: [ ] The firewall or gateway rules per conduit, with the date of the last review · [ ] The list of flows each rule allows, matched to the diagram

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

Z3 · OT apart from IT and from the Internet *(IMO Rev.4 3.5.3.3 · 33 CFR 101.650(e) and (h))*

What to check: No crane or yard equipment network is reachable from the office network or from the Internet except through the documented conduits; any OT system reachable from outside has a written justification.

Why: IMO Rev.4 asks to segment OT device networks from IT networks and to limit exploitable services on the Internet (3.5.3.3). For US facilities, 33 CFR 101.650 requires segmentation between IT and OT networks, logging and monitoring of all IT-OT connections, and a documented justification for any remotely accessible OT system.

Evidence to hold: [ ] The network diagram showing the OT zones separated from IT · [ ] The result of the last external exposure check, with its date · [ ] The justification for each OT system reachable from outside

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

Z4 · Yard radio networks treated as a separate segment *(NIST SP 800-82r3 6.2.9)*

What to check: The wireless network that serves the yard cranes, straddle carriers and other mobile machines is its own segment, with its own conduit to the rest of the OT; a site survey has checked coverage and where the signal leaks beyond the terminal.

Why: NIST recommends placing devices that use wireless communication in a separate network segment and performing a wireless survey before installation, noting that attackers use directional antennas to reach a network beyond its standard range (6.2.9).

Evidence to hold: [ ] The segment and conduit of the yard wireless network in the zone model · [ ] The latest wireless survey, with its date

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

Z5 · Electrical rooms, cabins and ports physically closed ***(33 CFR 101.650(i))***

What to check: Access to the e-houses, electrical rooms and control cabinets of the cranes is limited to authorised people and logged; unused network and USB ports on the machines are blocked, disabled or removed.

Why: For US facilities, 33 CFR 101.650(i) requires limiting physical access to OT and related IT equipment, securing and logging access to HMIs and other hardware, and blocking, disabling or removing unused physical access ports.

Evidence to hold: [ ] The access list for e-houses and electrical rooms, and its log · [ ] The port-blocking procedure and its last check

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

R · Vendor remote access

Remote access by equipment suppliers is requested, justified, limited, authenticated, logged and switched off after use.

R1 · Every remote access path is known *(USCG notices, 23 Feb 2024 and 19 Nov 2024 · IMO Rev.4 3.5.3.8)*

What to check: The terminal knows every way a supplier can reach a crane or a yard machine from outside: VPNs, remote desktop tools, cellular modems or routers installed on the machine, and remote monitoring links. Paths nobody owns are removed.

Why: In its 2024 notices on ship-to-shore cranes, the US Coast Guard writes that such cranes may by design be « controlled, serviced, and programmed from remote locations ». IMO Rev.4 asks to consider the risks posed by third-party vendors, embedded systems and maintenance devices (3.5.3.8).

Evidence to hold: [ ] The list of remote access paths per machine class, with the supplier and the owner on the terminal side · [ ] The date of the last check for paths that are not on the list

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

R2 · Remote access requested, justified and limited *(NIST SP 800-82r3 6.2.10)*

What to check: A supplier asks before each remote session; the terminal enables the access for the stated job only, on the machines concerned, and disables it at the end.

Why: NIST asks for a process for requesting and enabling remote access, and says remote access should be provided only if justified and limited to what the business need requires (6.2.10).

Evidence to hold: [ ] The remote access procedure · [ ] The record of the last sessions: who, which machine, why, start and end

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

R3 · Named accounts and multi-factor authentication *(NIST SP 800-82r3 6.2.10 · IMO Rev.4 3.5.3.1-3.5.3.2)*

What to check: Each remote user of a supplier has a named account (no shared supplier login) and uses multi-factor authentication.

Why: NIST recommends considering multi-factor authentication for remote access to the OT (6.2.10). IMO Rev.4 asks for unique credentials for all users (3.5.3.1) and for multi-factor or continuous authentication (3.5.3.2).

Evidence to hold: [ ] The list of supplier accounts and their holders · [ ] The MFA setting of the remote access gateway

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

R4 · Remote access never bypasses safety or security controls *(NIST SP 800-82r3 6.2.10)*

What to check: A remote session cannot override an interlock, bypass a safety function or open a path that skips the zone boundaries; changes to a crane program made remotely follow the same approval as on-site changes.

Why: NIST: « Remote access should not circumvent or negate safety or security controls » (6.2.10).

Evidence to hold: [ ] The written rule on what a remote session may and may not change · [ ] The change records of the last remote program changes

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

R5 · The contract says how the supplier connects *(IMO Rev.4 3.5.3.8 · NIST SP 800-82r3 4.2.1, 6.1.5)*

What to check: The maintenance and service contracts of the cranes and yard equipment state how the supplier connects, how access is logged, how security updates and incidents are handled, and what happens to the access when the contract ends.

Why: IMO Rev.4 asks for policies on software and hardware supply chain security for critical systems (3.5.3.8). NIST covers supply chain risk management for OT (4.2.1 and 6.1.5).

Evidence to hold: [ ] The security clauses of each equipment service contract · [ ] The list of critical equipment suppliers and how each reaches the machines

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

P · Patching and maintenance

Patches are tested before they reach a crane, compensating controls cover what cannot be patched, maintenance laptops and media are controlled.

P1 · A written OT patch process *(NIST SP 800-82r3 6.2.11)*

What to check: The terminal has a documented process for crane and yard equipment updates: how advisories are watched, who decides, when a patch is applied, how it is tested, and which compensating control is used while it waits.

Why: NIST asks for a systematic, accountable and documented OT patch management process covering how to monitor for patches, when to apply them, how to test them and how to select compensating controls when patching is delayed (6.2.11).

Evidence to hold: [ ] The OT patch procedure, dated and owned · [ ] The list of open advisories per machine class and the decision taken for each

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

P2 · Patches tested before they reach a working machine *(NIST SP 800-82r3 6.2.11)*

What to check: A patch or firmware update is tested on a test bench, an offline component or with the supplier, with regression tests, then installed in a planned maintenance window, one machine first.

Why: NIST: patches should be adequately tested, for example on offline systems, and regression testing is advised; a patch may remove a vulnerability but introduce a greater risk from a production or safety perspective (6.2.11).

Evidence to hold: [ ] The test record of the last patches installed · [ ] The maintenance window plan

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

P3 · Unsupported systems have compensating controls *(NIST SP 800-82r3 6.2.11)*

What to check: Each component that can no longer be patched (an operating system or a controller out of support) is listed, with the compensating controls that protect it (stricter zone, no remote access, monitoring) and a replacement plan.

Why: NIST notes that many OT systems use older operating systems no longer supported by the vendor, so patches may not be available, and points to compensating controls (6.2.11).

Evidence to hold: [ ] The list of unsupported components and their compensating controls · [ ] The replacement plan, with the planned dates

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

P4 · Maintenance laptops and media controlled *(NIST SP 800-82r3 6.2.5, 6.2.7 · IMO Rev.4 3.5.3.5)*

What to check: The laptops and tools used to program the cranes stay in the OT environment or are checked before use, run only approved software obtained from the supplier, and are disconnected after the job. USB keys and other media are controlled before they touch a machine.

Why: NIST recommends approved maintenance software with verified authenticity, limiting the use of maintenance devices outside the OT, and disconnecting any device and temporary connection after maintenance (6.2.5); it also covers removable media (6.2.7). IMO Rev.4 asks for controls against unauthorised removable media (3.5.3.5).

Evidence to hold: [ ] The list of maintenance laptops and who holds them · [ ] The removable media rule and the technical control in place

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

P5 · Configuration checked after maintenance *(NIST SP 800-82r3 6.2.5)*

What to check: After maintenance or an update, the configuration of the component is compared with its approved state, and any feature that was switched back on is switched off again.

Why: NIST: device configuration should be verified after maintenance and software patching, as some features may have been re-enabled or new features installed (6.2.5).

Evidence to hold: [ ] The approved configuration per component type · [ ] The post-maintenance check in the work order

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

S · Safety never depends on IT

Emergency stops, interlocks and limit protections keep working, and the machine goes to a safe state, whatever happens on the network.

S1 · Safety functions work without the network *(NIST SP 800-82r3 2.3.7, 4.2.2)*

What to check: Emergency stops, overload and limit protections, anti-collision and the other safety interlocks of each machine act locally, through the safety controller and hard-wired circuits, and do not need the TOS, the office network, the yard radio or any remote link to work.

Why: NIST describes safety systems as often independent from the other control systems, so that a failure of the control system does not affect them (2.3.7), and asks organisations to ensure adequate separation when control and safety are combined (4.2.2).

Evidence to hold: [ ] The list of safety functions per machine class and how each is implemented · [ ] Confirmation, from the supplier or the engineering file, that none depends on an IT link

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

S2 · A known safe state on loss of communication *(NIST SP 800-82r3 5.3.1)*

What to check: For each machine class, it is written what happens when the network or the radio link drops: the machine stops in a safe state, and the thresholds for degraded operation are defined.

Why: NIST: OT systems typically use fail-safe design, loss of network communications can trigger fail-safe events, and organisations should define the thresholds at which components can operate with reduced or disrupted capabilities (5.3.1).

Evidence to hold: [ ] The documented behaviour on loss of communication per machine class · [ ] The result of the last test, done in a maintenance window

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

S3 · Physical separation where safety requires it *(NIST SP 800-82r3 5.3.1)*

What to check: Where the safety assessment requires it, safety controllers sit on a physically separate network, not only a logical one (VLAN).

Why: NIST: safety considerations may require physical separation as opposed to logical separation (5.3.1).

Evidence to hold: [ ] The decision, per machine class, on physical or logical separation of the safety layer

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

S4 · Cyber and safety assessments talk to each other *(NIST SP 800-82r3 4.2.2)*

What to check: The people who run the crane safety assessments and those who run the cyber risk assessment share their results, and every new security control is checked for its effect on the safety functions before it goes live.

Why: NIST asks to consider the safety assessment results in the security risk assessment, and to evaluate the impact of security controls on the safety system (4.2.2).

Evidence to hold: [ ] The last joint review of cyber and safety risks for the equipment · [ ] The safety impact check of the last security change

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

D · Detect and recover

Watch the IT-OT connections, keep the programs and configurations backed up, know how to run and restart without the network.

D1 · IT-OT connections logged and watched *(33 CFR 101.650(h) · IMO Rev.4 3.5.4)*

What to check: Every connection between the office or TOS networks and the equipment networks, and every remote session, is logged, and someone reviews the logs.

Why: For US facilities, 33 CFR 101.650(h) requires that all connections between IT and OT systems are logged and monitored. IMO Rev.4 asks to monitor systems for relevant threats (3.5.4).

Evidence to hold: [ ] Where the logs of the conduits and remote sessions are kept, and for how long · [ ] The last review, with its date and who did it

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

D2 · Programs and configurations backed up and restorable *(NIST SP 800-82r3 3.3.9 · IMO Rev.4 3.5.3.7)*

What to check: The PLC programs, drive parameters, HMI projects and network configurations of each machine are backed up at a set interval and after each change, a copy is kept out of reach of the network, and a restore has been tested.

Why: NIST asks for backups of the OT systems' state, data, configuration files and programs at regular intervals, and for processes to restore them in a timely manner (3.3.9). IMO Rev.4 asks for regular backups (3.5.3.7).

Evidence to hold: [ ] The backup list per machine and the date of the last backup · [ ] The report of the last restore test

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

D3 · Running and restarting without the network *(NIST SP 800-82r3 3.3.9)*

What to check: The incident plan says how cranes and yard equipment are run, or safely stopped, when the TOS or the equipment network is lost, and in what order they restart, safety first.

Why: NIST: the recovery capability should prioritise human and environmental safety before restarting the OT operation that was impaired (3.3.9).

Evidence to hold: [ ] The equipment section of the incident response and continuity plans · [ ] The last exercise that used it (see the tabletop exercise kit)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

Sources (public, dated)

NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security, September 2023. https://csrc.nist.gov/pubs/sp/800/82/r3/final

IMO, MSC-FAL.1/Circ.3/Rev.4, Guidelines on maritime cyber risk management, 28 May 2026. https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.4.pdf

eCFR, 33 CFR 101.650, Cybersecurity measures (US Coast Guard rule), in force since 16 July 2025, read on 11 November 2026. https://www.ecfr.gov/current/title-33/chapter-I/subchapter-H/part-101/subpart-F/section-101.650

Federal Register, US Coast Guard notice of availability of MARSEC Directive 105-4 on ship-to-shore cranes (89 FR 13726), 23 February 2024. https://www.govinfo.gov/content/pkg/FR-2024-02-23/html/2024-03822.htm

Federal Register, US Coast Guard notice of availability of MARSEC Directive 105-5 on ship-to-shore cranes, 19 November 2024. https://www.govinfo.gov/content/pkg/FR-2024-11-19/html/2024-26896.htm

ISA/IEC 62443 series of standards (general reference, no text reproduced), overview page read on 11 November 2026. https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

Licence

Creative Commons Attribution 4.0 International (CC BY 4.0), https://creativecommons.org/licenses/by/4.0/ . You may copy, adapt and share this checklist, including commercially, if you credit Port Cyber Alliance and link to https://portcyberalliance.org/who-we-protect/terminal-operators/ot-security-cranes-yard/ . Generic: no terminal, port, client or vendor is named and no figure is invented. ISA/IEC 62443 is cited as a general reference; none of its text is reproduced. This checklist is not legal or engineering advice, does not replace the equipment supplier's documentation or the terminal's safety assessments, and must never be tested on a working machine. Port Cyber Alliance does not certify or audit terminals.