



OTSEC CANADA

OT SECURITY CANADA INDUSTRIAL CYBERSECURITY RISK ASSESSMENT

NIST SP 800-82r4 + UNEP Environmental Impact Overlay | Security, resilience and operational efficiency

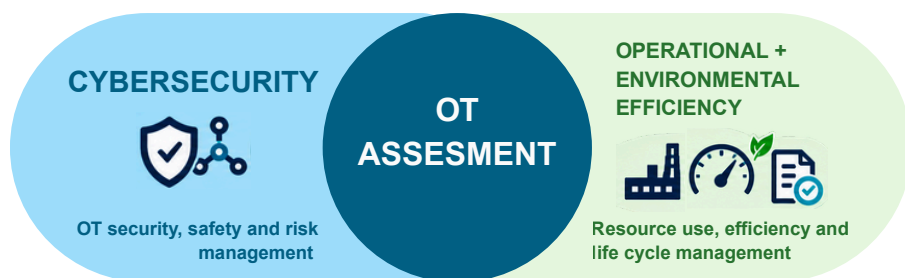


SECURE OPERATIONS.
RESILIENT PRODUCTION.
LOWER ENVIRONMENTAL IMPACT.



ONE ASSESSMENT CAN SUPPORT TWO MANAGEMENT PRIORITIES

The overlap is practical. NIST SP 800-82r4 connects OT security with safety, efficiency and environmental impact, and calls for relevant environmental obligations to be considered in OT governance. UNEP adds an environmental lens for digital and AI systems: measure direct resource impacts, design for sustainability, improve computational efficiency, and manage hardware through its full life cycle. Together, these practices allow OTSEC to assess security controls while also identifying opportunities to reduce energy, water, waste and unnecessary equipment replacement.



COMBINED CONTROL PRIORITIES



GOVERN CYBER + ENVIRONMENTAL RISK

Extend the OT risk register to capture safety consequences, environmental consequences, energy or water dependencies, and AI/cloud dependencies. Use one executive governance process for cyber, operations and environmental obligations.



INVENTORY + LIFE-CYCLE MANAGEMENT

Inventory PLCs, HMIs, IIoT, BACS, cloud services and AI-enabled functions. Track support status and critical dependencies. Decommission securely, retain chain of custody, and handle hazardous devices or e-waste appropriately.



MONITOR SECURITY + RESOURCE PERFORMANCE

Use trusted OT telemetry and baselines to detect cyber anomalies while also measuring useful operating indicators such as energy use, water use, equipment condition and abnormal process consumption where sensors support it.



SECURE EFFICIENCY TECHNOLOGIES

Protect smart HVAC, energy management, predictive maintenance, renewable-energy balancing and AI-enabled controls with segmentation, least privilege, MFA, controlled remote access and tested recovery.



ASSURE SUPPLIERS + CLOUD / AI SERVICES

Expand vendor assurance beyond remote access and patching. For AI and cloud services, request practical evidence about life-cycle support, energy or resource metrics, data-centre practices and end-of-life handling where material.



DESIGN FOR SAFE, EFFICIENT RESILIENCE

Test graceful degradation, local control, manual fallback and recovery. Resilient operation can limit the safety, production and environmental consequences of a cyber incident or failed external service.

NEW ENVIRONMENTAL NORMS

UNEP 2024 recommendations for digital and AI systems



- **Measure direct impacts:** energy, water, material use, greenhouse-gas emissions and e-waste.
- **Make metrics visible:** request useful environmental data from relevant AI, cloud and digital suppliers.
- **Use sustainability by design:** include resource consumption in new or changed digital and AI components.
- **Prefer efficient AI:** reduce unnecessary computation, data use and inference demand where practical.
- **Prefer lower-impact infrastructure:** efficient data centres and renewable energy where suitable.

Important: UNEP notes that no standardized global measurement method exists yet. Treat these as assessment and procurement criteria, not certification or legal compliance.

BENEFITS OF THE COMBINED PRIORITIES



More secure: fewer unmanaged connections, stronger vendor controls and better anomaly detection.



More resilient: safer fallback, clearer dependencies and faster recovery.



More efficient: better asset visibility, predictive maintenance and less avoidable downtime.



Lower-impact operations: potential reductions in wasted energy and water, premature replacement and e-waste.



Better evidence: one management-ready record can support cyber assurance, operational risk and environmental reporting conversations.

OTSEC CANADA: INTEGRATED INDUSTRIAL CYBERSECURITY + ENVIRONMENTAL EFFICIENCY LENS

Applied within the Industrial Cybersecurity Risk Assessment: scope critical processes | inventory OT, IIoT and AI/cloud dependencies | map segmentation and remote access | review safety and environmental consequences | validate telemetry | assess suppliers | test fallback and recovery | issue one prioritized remediation roadmap.

Result: Protect production and safety while identifying defensible opportunities for resilience, efficiency and a lower environmental footprint.

Sources: NIST SP 800-82r4 ipd, Guide to Operational Technology (OT) Security, Initial Public Draft, September 2026; UNEP, Artificial Intelligence (AI) end-to-end, 2024. NIST is draft guidance and UNEP is an issues note, not a certification standard. | OTSEC Canada by Datarisk Canada, Informatica Group | www.OTSEC.ca



OTSEC CANADA

OT SECURITY CANADA INDUSTRIAL CYBERSECURITY RISK ASSESSMENT

NIST SP 800-82r4 + UNEP Environmental Impact Overlay | Security, resilience and operational efficiency

READY TO VERIFY YOUR OT SECURITY PROGRAM?

Request a no-charge industrial cybersecurity consultation with OTSEC Canada.

A qualified OT cybersecurity advisor will discuss your industrial environment, current controls, applicable standards and the areas you want independently reviewed. The consultation is confidential and there is no obligation to proceed.

ORGANIZATION: <i>Click or type here</i>	FACILITY / SITE: <i>Click or type here</i>
CONTACT NAME: <i>Click or type here</i>	TITLE / ROLE: <i>Click or type here</i>
EMAIL: <i>Click or type here</i>	PHONE: <i>Click or type here</i>
INDUSTRY/ SECTOR: <i>Click or type here</i>	PROVINCE / REGION: <i>Click or type here</i>
PRIMARY CONCERN / OBJECTIVE: <i>Click or type here</i>	TIMING: <i>Click or type here</i>

CONSULTATION FOCUS
☐ OT / ICS risk assessment ☐ Compliance readiness ☐ Vendor / remote access ☐ Incident response ☐ Cloud / IIoT / AI ☐ Environmental efficiency
WHAT WOULD YOU LIKE OTSEC TO REVIEW?

WHAT WOULD YOU LIKE OTSEC TO REVIEW?

OTSEC CYBERSECURITY COMPLIANCE CHECKLIST

Check “In place” for controls you believe are implemented.
Check “Verify” for items you want OTSEC Canada to independently test, evidence or map to applicable requirements.

CONTROL OR SAFEGUARD	IN PLACE	VERIFY
Governance and risk register: OT ownership, accountable roles, risk criteria, business/safety consequences and tracked risk treatment.	☐	☐
OT asset inventory and criticality: Hardware, software, PLCs, HMIs, IIoT, BACS, connections, dependencies, support status and critical functions.	☐	☐
Secure architecture and segmentation: Defined IT/OT boundaries, DMZs, firewalls or other appropriate separation; documented network paths.	☐	☐
Identity, authentication and remote access: Least privilege, separate OT credentials where appropriate, MFA for remote access, controlled vendor access and session accountability	☐	☐
Configuration, patching and hardening: Secure baselines, tested patches/firmware, disabled unnecessary ports/services, protected engineering workstations and change control.	☐	☐
Monitoring, logging and anomaly detection: Network/device monitoring, time synchronization, audit trails, baselines and escalation for suspicious or abnormal activity	☐	☐
Backup, resilience and recovery: Tested backups, redundancy, graceful degradation, local/manual , fallback and safe restoration of physical processes.	☐	☐
OT incident response and exercises: OT-specific response/recovery playbooks, communications, vendor roles, tabletop exercises and lessons learned.	☐	☐
Supply-chain and vendor assurance: Security requirements, supplier vetting, remote-maintenance controls, lifecycle support, vulnerability handling and end-of-support planning.	☐	☐
Cloud, IIoT and AI governance: Shared responsibilities, strong boundaries, data governance, logging, availability dependencies and safe local fallback for critical functions.	☐	☐
Safety, environmental and resource performance: Cyber risk considers safety/environmental consequences; trusted telemetry can support energy/water monitoring, predictive maintenance and responsible decommissioning.	☐	☐
Applicable standards and evidence mapping: Relevant obligations and standards identified and evidenced, including NIST SP 800-82r4 / CSF 2.0, IEC 62443, NERC CIP, ISO 27001, UL 2900 or sector requirements where applicable.	☐	☐

OTSEC CANADA: INTEGRATED INDUSTRIAL CYBERSECURITY + ENVIRONMENTAL EFFICIENCY LENS

Applied within the Industrial Cybersecurity Risk Assessment: scope critical processes | inventory OT, IIoT and AI/cloud dependencies | map segmentation and remote access | review safety and environmental consequences | validate telemetry | assess suppliers | test fallback and recovery | issue one prioritized remediation roadmap.

Result: Protect production and safety while identifying defensible opportunities for resilience, efficiency and a lower environmental footprint.

Sources: NIST SP 800-82r4 ipd, Guide to Operational Technology (OT) Security, Initial Public Draft, September 2026; UNEP, Artificial Intelligence (AI) end-to-end, 2024. NIST is draft guidance and UNEP is an issues note, not a certification standard. | OTSEC Canada by Datarisk Canada, Informatica Group | www.OTSEC.ca