



IEC 62443, OT Cyber Risk and Cyber Insurance

How to lower insurance premiums through
better OT security



IDENTIFY
ASSETS



ASSESS
RISKS



EVALUATE
CONTROLS



TREAT &
PRIORITIZE
RISKS



MONITOR &
IMPROVE

This page has been intentionally left blank

About this paper

This paper asks a narrower and harder question than most writing on the subject. It does not assume that IEC 62443 compliance lowers cyber-insurance premiums. It asks whether, when and through which mechanisms IEC 62443-aligned controls can influence how an insurer sees, terms and prices an industrial operator, and it reports plainly where public evidence stops.

How evidence is labelled

Statements that carry weight are tagged so that the reader can see what kind of support they have. The tags are used at paragraph level and in tables.

Tag	Meaning	How to treat it
DOCUMENTED FACT	Published by a primary source: a standard, regulator, insurer, court record or company disclosure	Reliable for what it states; check date and scope
INDUSTRY PRACTICE	Widely reported market or engineering practice, not tied to a single primary source	Directionally reliable; verify against your own policy and broker
RESEARCH FINDING	Result of an empirical or modelling study, with stated method and period	Read with the study limits noted in the text
INSURER / UNDERWRITER PERSPECTIVE	A view attributed to an insurer, broker or underwriting specialist	One participant view; not a market-wide rule
REASONED ANALYSIS	The author's inference from the evidence above	Plausible and testable; not established fact
EMERGING PRACTICE / HYPOTHESIS	Early or vendor-reported practice, or an untested proposition	Do not plan budgets around it

Ground rules followed

- No insurance discount, underwriting formula or insurer requirement is stated unless a source is cited. Where the evidence for a link is thin, the text says so.
- Quantitative claims carry a source and date. Studies are described with their period and scope so that older or IT-centred results are not read as current OT findings.
- Standards are described at part and topic level. No clause numbers are cited; readers should consult the published texts.
- Illustrative figures are labelled as assumptions. They are not insurer pricing and no insurer has reviewed them.
- Where sources disagree, both positions are presented and attributed.

NOTICE | Classification of cited threat data

Sections 5 and 9 draw on statistics from the Shieldworkz H1 2026 OT Threat Advisory (28 May 2026, marked TLP:AMBER). This document therefore carries TLP:AMBER until the cited figures are cleared for wider release; it can then be re-marked TLP:CLEAR.

Executive summary

What the evidence supports

- **Premium drivers in public research are mostly not security controls.** The best-known academic content analysis of US cyber policy filings found premium calculation dominated by exposure measures such as revenue rather than control maturity . It predates OT-specific underwriting and is IT-centred.
- **The market cycle dominates headline pricing.** Marsh reported global cyber rates falling for a twelfth consecutive quarter in Q2 2026 . Any observed premium fall is therefore hard to attribute to a control programme.
- **OT losses are large, mostly indirect and only partly insured.** Norsk Hydro reported a 2019 impact of NOK 650 to 750 million, with insurance compensation of NOK 220 million recognised by year end. The Cyber Monitoring Centre modelled the 2025 Jaguar Land Rover incident at about GBP 1.9 billion.
- **Practitioner views conflict.** Some insurance and risk specialists report that strong OT controls improve terms and capacity; others regard the incentives as weak or inconsistent. This paper reports both.

What it does not support

- That an IEC 62443 certificate produces a quantified discount.
- That insurers treat the presence of a certificate as a substitute for evidence about the underlying controls.
- That the illustrative financial model in Section 11 approximates any insurer's pricing. It does not.

What we recommend

- Treat IEC 62443 as a structured method for identifying, managing and demonstrating OT cyber risk, and build an evidence pack an underwriter can inspect (Figure 6).
- Quantify residual OT exposure in financial terms and test it against limits, retentions and exclusions. In the illustrative model the tail, not the expected annual loss, is the material exposure.
- Approach the insurer through the broker with dated, scoped evidence and an explicit list of gaps and remediation dates.
- Use the 90-day roadmap in Section 13 to establish visibility, close priority gaps and assemble the pack.

1. Purpose and scope

Industrial cyber risk sits awkwardly in insurance. Policies were built around data breach and IT disruption; industrial losses arise from production stoppage, physical process consequences and dependence on long-lived control systems. Operators are increasingly asked what they are doing about OT security, and security teams are increasingly asked whether the investment will reduce insurance cost. This paper examines that second question with the evidence available in September 2026.

It is written for CISOs, OT and ICS security leaders, plant security leaders, operational technology executives, risk and insurance managers, and senior decision-makers. It covers IEC 62443 in an insurance context, how insurers may assess OT risk, the economics of OT loss, a control-to-underwriting mapping, the state of evidence on premiums, sector differences, a readiness framework, an illustrative business case and a 90-day plan.

Sources and method

Sources were prioritised in this order: standards bodies and their public documentation; insurer, broker and reinsurer publications (Marsh, Munich Re, Lloyd's); regulator and company disclosures; peer-reviewed research; specialist industry research; and trade-press reporting of practitioner views. Vendor material, including the publisher's own, is used only for what it can establish and is labelled as such. Publication dates are shown so that older research is not read as current. Search for named insurers that publicly credit IEC 62443 in rating or filing documents found none; that absence is reported as a limit, not as proof that none exists.

LIMITS | What this paper cannot do

It cannot state what any insurer will do for any operator. Underwriting models, risk appetite, loss history and policy wording are insurer-specific and largely not public.

It cannot substitute for the operator's own broker, policy wording or legal advice.

2. The core question

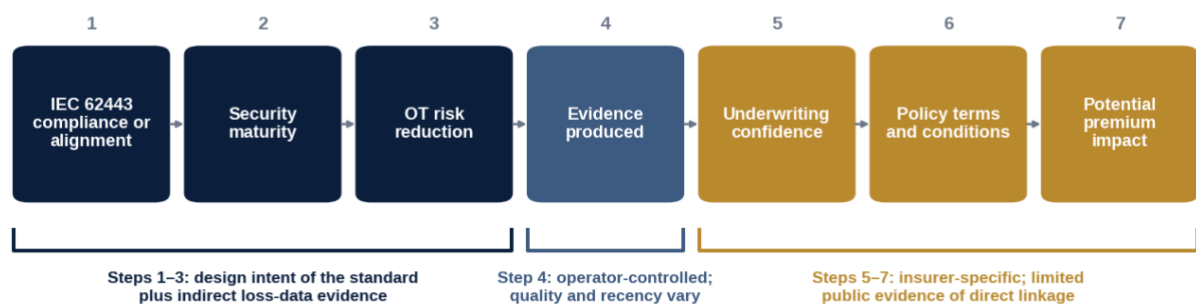
The question in the title contains two claims that are often collapsed into one:

THE CORE QUESTION

Does IEC 62443 compliance itself reduce cyber-insurance premiums, or does the security maturity demonstrated through IEC 62443-aligned controls influence how insurers perceive and price OT cyber risk?

Figure 1 · From IEC 62443 to underwriting: a chain of related, not interchangeable, steps

Evidence strength weakens as the chain moves from the operator's environment toward the insurer's pricing model



How to read this chain

- Compliance is a statement about conformity. Maturity is what the organisation can actually do. Risk reduction is a change in loss likelihood or severity.
- Underwriters price expected loss and their own uncertainty about it. Evidence is what narrows that uncertainty.
- A certificate or assessment can support the chain only where it is backed by current, inspectable evidence of the underlying controls.
- Premium is the last link and is set by the insurer's model, appetite and market cycle, not by the operator.

Source: author's analytical framework. Evidence-strength grouping reflects the availability of public evidence discussed in Sections 2 and 7.

Seven steps that are related but not interchangeable

Step	What it is	Who controls it	Evidence position
1. Compliance or alignment	Conformity with requirements of the IEC 62443 series, in whole or part, at a stated scope	Operator and assessor	Scope and rigour vary widely; a claim of "62443 compliant" is meaningless without scope, levels and date
2. Security maturity	What the organisation actually does and can do, consistently, under operating pressure	Operator	Observable only through evidence and testing
3. Risk reduction	Lower likelihood or severity of loss events	Operator, adversary behaviour	Indirect evidence: claims-based model; incident post-mortems
4. Evidence	Current, inspectable artefacts that demonstrate steps 1 to 3	Operator	Quality, recency and scope determine usefulness
5. Underwriting confidence	The insurer's reduced uncertainty about the risk	Insurer	Limited public evidence of how OT evidence is weighted
6. Policy terms and conditions	Coverage, retentions, limits, conditions, sub-limits, exclusions	Insurer, negotiated through the broker	Documented practice is thin for OT; see Section 8

Step	What it is	Who controls it	Evidence position
7. Potential premium impact	Price of the risk transferred	Insurer, market cycle	No direct evidence linking IEC 62443 to a pricing variable; see Section 7

Why insurers may care about controls more than certificates

REASONED ANALYSIS An underwriter prices expected loss and the uncertainty around it. A certificate says something was assessed against a standard at a scope and date. It says little about whether remote access is currently controlled, whether backups restore, or whether the plant that was not in scope is exposed. Underwriters who ask OT-specific questions are asking about those facts. Where an IEC 62443 assessment produces an asset register, zone model, target security levels and a gap register, it produces the kind of evidence that reduces uncertainty. Its value is in that evidence, not in the label.

INSURER / UNDERWRITER PERSPECTIVE Practitioners on an industry panel described insurers as interested in demonstrated controls and in visibility of OT environments rather than in framework names alone. A vendor describing its own underwriting methodology reports that unanswered OT questions can be treated as risk signal. Both are single-source perspectives and should be read as such.

The conclusion of this section is structural: the chain in Figure 1 can be strong at steps 1 to 4, which the operator controls, and uncertain at steps 5 to 7, which the insurer controls. Most of the value an operator can capture is by making step 4 excellent.

3. IEC 62443 through an insurance lens

IEC 62443 is a series of standards for the security of industrial automation and control systems (IACS), developed jointly in the IEC and ISA communities. It is organised by role: asset owners, service providers, system integrators and product suppliers. This section does not tutor the standard. It states what each part contributes that an insurer could observe or use.

The parts that matter most for insurance discussions

Part	Addresses (topic level)	Insurance-relevant contribution
IEC 62443-2-1	Security programme for IACS asset owners: governance, policies, roles, risk management, lifecycle. A revised edition was published in 2024 [20]	Evidence of security governance, accountability and a managed programme rather than ad hoc controls
IEC 62443-2-4	Security programme requirements for IACS service providers, including integrators and maintenance	Supplier and vendor assurance; visibility of third-party access practices
IEC 62443-3-2	Security risk assessment and system design: system under consideration, zones and conduits, target security levels	Structured OT risk assessment; documented segmentation logic; the closest the standard comes to an OT loss-scenario view
IEC 62443-3-3	System security requirements and security levels, organised by seven foundational requirements	A checkable list of technical capabilities; basis for stating achieved versus target levels
IEC 62443-4-1	Secure product development lifecycle for suppliers	Supplier maturity; relevant when insuring against product-originated vulnerabilities
IEC 62443-4-2	Technical security requirements for IACS components	Component-level capability; informs what compensating controls are needed for legacy devices

Source for structure and scope: IEC and ISA public documentation of the series and secondary technical summaries [20][22]. Readers should consult the published texts for normative wording.

Concepts, translated into risk visibility and underwriting terms

Concept	Risk-visibility and risk-reduction effect	Why an underwriter might care
Security levels (SL-T, SL-C, SL-A)	Target, capability and achieved levels express how strongly a zone must resist an assumed class of attacker and how far it currently does. A gap between target and achieved is a quantified statement of exposure	A consistent vocabulary for stating what protection exists relative to need; a target is a risk decision, not a discount tier
Zones and conduits	Group assets by function and consequence; define and control the communication paths between them. Limits lateral movement and defines blast radius	Bears directly on severity: whether an IT compromise can reach production and how far
Foundational requirements (identification and authentication control, use control, system integrity, data confidentiality, restricted data flow, timely response to events, resource availability)	A structured frame for technical controls across seven categories	Allows control coverage to be described completely rather than by selected highlights
Risk assessment and asset identification	You cannot assess or defend what is not inventoried. Asset identification and consequence analysis define scope and priority	Visibility is the first uncertainty an underwriter faces
Access control and secure remote access	Limits credential misuse and vendor-path compromise; supports accountable, logged access	Third-party and remote paths are a common route into OT environments
System hardening and malware protection	Reduces attack surface on engineering workstations, HMIs and servers	Affects likelihood of initial compromise and spread

Concept	Risk-visibility and risk-reduction effect	Why an underwriter might care
Patch and vulnerability management	In OT, a disciplined process that prioritises, tests and, where patching is impractical, compensates	Evidence of remediation discipline for legacy and unsupported systems
Incident response and recovery	OT-specific plans, roles and exercised recovery reduce downtime	Business-interruption duration is a major loss driver; incident response planning shows the largest modelled reduction
Security governance	Roles, policy, review cycles, metrics, management accountability	Indicates whether controls persist beyond a project
Secure product development and supplier security	Suppliers build and maintain products to a defined lifecycle; operators specify supplier obligations	Third-party and supply-chain risk are underwriting themes across cyber lines

SCOPE OF CERTIFICATION

Certification under recognised IEC 62443 schemes has historically applied to products, processes and, in some schemes, systems and service providers. It is not a single certificate that attests to an operator's whole environment. An insurer or broker reading a claim of "IEC 62443 certification" should ask what was certified, by which body, at which security level, for which scope and when [20].

4. How cyber insurers assess OT risk

Public evidence on how insurers assess OT risk is uneven. Much of what is documented concerns IT-centred questions (multi-factor authentication, endpoint detection, backups, incident response) that are also relevant to OT. OT-specific underwriting is developing; practitioners on a 2025 panel described a gap between how much OT-derived loss potential exists and how granular the underwriting information is, and a specialist vendor reports OT-specific questionnaires and analytics entering us.

INDUSTRY PRACTICE Industry practice reported across the market: underwriters typically gather information through application forms and questionnaires, sometimes supplemented by external scans, broker discussions and, for larger risks, calls with security leadership. Questions on IT controls are standardised; OT content is less consistent. Research on proposal forms has documented substantial variation in which controls forms ask about.

The table below organises the areas an underwriter may examine for an industrial operator and shows where IEC 62443 can provide structured evidence. It describes what insurers may ask, not what any specific insurer does.

Area an insurer may examine	What the underwriter is trying to learn	Where IEC 62443 can provide structured evidence	Basis
OT asset visibility; critical asset identification	Is the exposure known and scoped?	Asset identification and system-under-consideration definition (2-1, 3-2)	Analysis;
IT/OT segmentation; network architecture; industrial protocols	Can an IT compromise reach production? What is exposed?	Zone and conduit design and documented permitted flows (3-2, 3-3)	Analysis;
Remote access; privileged access; third-party and vendor access	Who can reach OT, how, with what accountability?	Access control and remote-access requirements; service-provider requirements (3-3, 2-4)	Practice;
Vulnerability and patch management; legacy and unsupported systems	How does the operator manage weakness it cannot patch?	Programme requirements and compensating-control logic (2-1, 3-3, 4-2)	Analysis
Monitoring, detection and SOC capability	How quickly would an intrusion be seen below the IT/OT boundary?	Timely-response-to-events foundational requirement (3-3); monitoring coverage evidence	Practice;
Backup, recovery, business continuity, disaster recovery, ransomware resilience	How long could production be down and can it be restored?	Resource availability and recovery practice; programme requirements (2-1, 3-3)	Practice;
Incident response	Is there an exercised OT plan with decision rights?	Incident and recovery requirements in programme and system parts	Practice;
Identity and access management	Are credentials controlled and monitored?	Identification and authentication control; use control (3-3)	Practice
Security governance; security maturity evidence; testing	Does the programme persist and improve?	Security management system requirements (2-1); assessment records	Analysis
Supply-chain risk	How exposed is the operator to supplier compromise or outage?	Service-provider and product-supplier parts (2-4, 4-1, 4-2)	Practice
Regulatory compliance	Are legal obligations understood and met?	Mappings from sector regulation to 62443 exist in some sectors	Analysis

CAUTION | IEC 62443 is evidence-shaped, not underwriter-shaped

IEC 62443 was written to secure control systems, not to feed rating models. Its outputs (zone models, security level targets, gap registers) are useful evidence, but an underwriter must be able to read them. Operators should be prepared to summarise them in the terms of the underwriter's question, and to expect that some insurers will still rely mainly on IT-derived questionnaires.

5. The insurance economics of OT cyber risk

The economic logic runs in a chain: cyber exposure, probability of an incident, operational impact, expected loss, insurability, underwriting, coverage and terms, and finally premium. Controls can act on the early links. The later links belong to the insurer.

Why OT losses differ from conventional IT breach losses

Loss component	OT characteristic	Note
Production shutdown and business interruption	Loss accrues per day of lost output and can dwarf data-breach costs	JLR: modelled at about GBP 1.9bn, largely lost manufacturing output after an incident that began in IT [7]
Safety implications	Process upset or unsafe state	Not a standard cyber-policy peril; may sit outside cyber wording
Equipment damage; physical consequences	Manipulation of controllers or safety systems can damage assets	Rare but severe; ambiguity between cyber and property cover is a recognised issue [2]
Environmental impact	Releases or discharges linked to process control failure	Liability may fall under other policies
Supply-chain disruption	Downstream customers and upstream suppliers are interrupted	Contingent BI; cascades beyond the operator
Regulatory consequences	Sector regulators, critical-infrastructure and data laws	Fines and sanctions may be uninsurable in some jurisdictions
Recovery, rebuild and forensic costs	Rebuilding engineering workstations, re-validating processes	Norsk Hydro operated manually for weeks and reported a NOK 650 to 750M full-year impact
Reputational and customer impact	Contract penalties, lost orders	Frequently excluded or hard to measure

DOCUMENTED FACT Norsk Hydro (March 2019, LockerGoga ransomware) reported a full-year 2019 impact of NOK 650 to 750 million, with insurance compensation of NOK 33 million recognised in the third quarter and NOK 187 million in the fourth, and further recoveries expected. On the mid-range impact that is roughly 30%, the author's arithmetic; the figure is not a general recovery rate.

DOCUMENTED FACT The Cyber Monitoring Centre assessed the 2025 JLR incident as a Category 3 event with a central estimate of about GBP 1.9 billion in economic impact. Merck's NotPetya-related claim of about USD 1.4 billion against its property insurers was contested on a war-exclusion argument and settled in 2024. A.P. Moller-Maersk reported NotPetya costs of about USD 300 million.

The threat context for industrial operators

RESEARCH FINDING Dragos reported that around 3,300 industrial organisations were affected by ransomware in 2025 and that the number of tracked ransomware groups targeting industrial organisations rose to 119. The Shieldworkz H1 2026 OT Threat Advisory (28 May 2026) reports a 77% rise in OT incidents in 2025, a 33% increase in physical disruptions in H1 2026, more than 19,000 internet-exposed ICS devices, and that 77% of OT attacks with physical impact entered through the IT network. The advisory is the publisher's own intelligence product and its methodology is not independently reviewed here.

The IT-origin finding matters for insurance: an operator whose OT is well segmented may still suffer a production stoppage from an IT-side event, through precautionary shutdown or dependence on IT-hosted scheduling and control software. Underwriters concerned with business interruption therefore have reason to ask about IT/OT boundary control as well as OT security in isolation.

Why demonstrably stronger controls may present a different risk

REASONED ANALYSIS Two operators with the same revenue, sector and asset value can present different expected losses if one can show that production networks are segmented, remote access is controlled, detection exists below the boundary, and recovery has been tested. The other cannot. The first has a narrower plausible range of outcomes, and its statement of that range can be checked. Whether an insurer reflects that in price depends on whether its model can see and credit it.

PRICING AUTHORITY

Premium is determined by the insurer from its own underwriting model, risk appetite, loss history, exposure information, reinsurance cost and policy-specific considerations. Market cycle is a major driver: Marsh reported global cyber rates declining for the twelfth consecutive quarter in Q2 2026, and Munich Re estimated global cyber premiums at roughly USD 15 billion in 2025 with slower growth.

6. IEC 62443 practices and potential underwriting relevance

The mapping below links major IEC 62443 practices to the OT risk they address, the evidence an operator can produce and the potential relevance to underwriting. It is analysis, not an insurer rating table. Figure 3 shows the same relationships as a matrix.

NOTICE | No implied discount

Nothing in the table implies that an insurer assigns a monetary discount to any control. Potential underwriting relevance describes how the evidence may help the insurer understand or narrow the risk.

IEC 62443 practice	OT risk addressed	Evidence an operator can produce	Potential underwriting relevance
Asset inventory and system definition	Unknown or unmanaged assets and exposure	Current OT asset register with owner, criticality, firmware and support status	Improved risk visibility; scope of the exposure is stated
Zones and conduits	Excessive connectivity; IT-to-OT propagation	Architecture diagrams, zone and conduit register, firewall and rule-set review records	Reduced lateral-movement exposure; narrower loss severity
Security levels (target, capability, achieved)	Protection not matched to consequence	Documented SL-T per zone; SL-A assessment; gap register	Demonstrates risk-based rather than uniform security
Access control and authentication	Credential misuse; unauthorised change	IAM and privileged-access records; MFA scope; account review logs	Reduced credential-related exposure
Secure remote and vendor access	Vendor or remote path compromise	Remote-access architecture, session logs, vendor access approvals	Reduced third-party attack surface
Hardening and malware protection	Exploitable configurations; malware spread	Hardening baselines, application allow-listing or equivalent, exception register	Lower likelihood of compromise and spread
Patch and vulnerability management	Exploitable OT weaknesses; unsupported systems	Vulnerability register, patch decisions, compensating controls for unpatched assets	Demonstrable remediation discipline; explanation of legacy exposure
Monitoring and detection	Undetected intrusion; long dwell time	OT monitoring coverage map, alert handling records, detection metrics	Improved detection capability; shorter potential loss window
Incident response	Slow containment; uncoordinated recovery	OT incident response plan, exercise reports, decision-rights matrix	Improved resilience; strongest modelled effect
Backup, recovery and continuity	Extended downtime; unrecoverable configurations	Backup scope for controllers and engineering files, restore test results, recovery-time evidence	Bears on business-interruption duration
Security governance and risk assessment (2-1, 3-2)	Ad hoc, project-based security	Policy set, risk assessment method and outputs, management review minutes, KPIs	Confidence that controls persist
Supplier and service-provider security (2-4, 4-1, 4-2)	Third-party compromise; insecure products	Supplier contract clauses, product security evidence, integrator assessment	Contains a supply-chain exposure theme

Figure 3 · IEC 62443-aligned practices mapped to insurance-relevant risk factors

Analytical mapping showing where each practice acts most directly; not an insurer rating table

	Likelihood of initial compromise	Lateral movement and loss severity	Detection and dwell time	Recovery time / BI duration	Third-party exposure	Evidence and transparency
Asset inventory and system definition	○	○	○	○		●
Zones and conduits (segmentation)	○	●	○	○	○	○
Target security levels (risk-based)	○	○			○	●
Access control and authentication	●	○	○		○	○
Secure remote and vendor access	●	○	○		●	○
Patch and vulnerability management (with compensating controls)	●	○			○	○
Monitoring and detection	○	○	●	○	○	●
OT-specific incident response		●	○	●		○
Backup, recovery and continuity		○		●		○
Supplier and product security	○				●	○

● Primary effect
 ○ Secondary effect
 Indirect or minimal

Source: author's reasoned analysis of how the practices named in IEC 62443 act on loss frequency, severity and evidence quality. Whether and how an insurer credits any cell is insurer-specific and is not established by public evidence.

7. Does IEC 62443 actually lower premiums?

This is the central question. The evidence is presented in four classes so that the reader can see how much of the popular claim survives scrutiny.

Direct evidence

Direct evidence would be an insurer, filing, rating manual or study showing IEC 62443 compliance or certification as a rating variable, with a stated effect on premium. **We did not find any public evidence of this kind.** Insurer rate filings and rating models are largely confidential, and OT-specific pricing is not visible in the public literature. Absence of public evidence is not evidence that no insurer does this; it is a limit on what can be claimed.

RESEARCH FINDING The most cited empirical work on cyber-insurance pricing analysed policy filings with US state regulators and found that premiums were driven mainly by exposure measures such as revenue rather than by security control maturity. The period studied predates OT-specific underwriting and the study is not about industrial risk. It shows how loosely security controls were reflected in pricing formulae at the time, not how OT risk is priced today.

REASONED ANALYSIS These controls correspond to practices IEC 62443 organises (architecture and zoning, access, monitoring, response). The study did not test IEC 62443 and does not show that standards compliance produces the modelled effects. The inference from the study to a standards-aligned programme is reasonable and has not been tested.

Emerging evidence

- **Panel perspectives (2025).** Industry specialists on a trade-press panel described OT security maturity and demonstrable controls as relevant to underwriting and capacity. Panellists also disagreed about how far premiums or terms currently reflect it, with some describing incentives as weak or inconsistent.
- **Underwriting tooling.** A specialist OT risk-quantification vendor reports insurers using OT-specific questionnaires, analytics tools that reference IEC 62443 and NIST SP 800-82, and at least one carrier as an early adopter. The source is a vendor describing its own market; treat as emerging practice.
- **Security vendor commentary.** TXOne Networks reported in 2025 that insurers have begun researching whether organisations meet frameworks such as NIST CSF and the IEC 62443 series. Trade press in late 2025 similarly reported insurer interest in adherence to NIST SP 800-82, IEC 62443 and CISA performance goals. Both are unnamed-insurer, secondary reports.
- **Shieldworkz position.** The publisher stated in July 2026 that underwriting has begun pointing directly to IEC 62443 as an accepted baseline for demonstrating due diligence. The article does not name insurers or documents, and we classify the statement as an emerging-practice claim consistent with but not independently substantiated in public sources.

Unsupported claims

The following claims recur in vendor and advisory content and are **not** supported by evidence we could find:

- "IEC 62443 certification lowers premiums" stated as a general rule.
- Specific percentage discounts attributed to IEC 62443, with no cited insurer, filing or study.
- That an IEC 62443 certificate replaces an insurer's own assessment or questionnaire.
- That insurers accept a single certificate as proof of security across an entire industrial estate.

- That premium reductions observed in 2024 to 2026 were caused by control investment rather than by the softening market.

Where the sources disagree

Question	View A	View B	Our reading
Do insurers reward OT security maturity today?	Insurers increasingly consider demonstrated controls and offer better capacity or terms where evidence is strong	Incentives are weak; underwriting of OT remains coarse and pricing is driven by market conditions	Both are partly right: evidence use is emerging and uneven, and market cycle masks control effects
Is a framework certificate meaningful?	Frameworks provide an accepted baseline and vocabulary	Insurers weight verified controls over labels	Certificates help only as an index to evidence
Is OT risk a cyber or property risk?	Cyber policies increasingly respond to OT-induced BI	Physical damage often sits with property policies and can conflict	Coverage architecture must be tested per policy

What can reasonably be inferred

REASONED ANALYSIS (1) IEC 62443-aligned controls plausibly reduce the loss drivers insurers price, on indirect evidence. (2) The route to insurance value is evidence quality and coverage clarity, which the operator controls. (3) Premium effect is real only where an insurer can observe the evidence and chooses to credit it; that is insurer-specific and currently undocumented in public sources. (4) Operators should plan for insurability, terms and residual exposure before planning for premium reduction.

8. Beyond premiums: the broader insurance value

Because pricing is the least evidenced link, the more defensible value case rests on other factors. The table separates documented industry practice from analytical interpretation.

Factor	Documented industry practice	Analytical interpretation for OT operators
Insurability and coverage availability	Insurers have declined or restricted risks with poor hygiene; the market has at times imposed conditions such as MFA and backups [14]	Operators unable to describe OT controls may find capacity narrower for OT-heavy exposures
Policy terms and conditions	Terms include limits, sub-limits, waiting periods, exclusions and conditions; state-backed cyber-attack exclusions are required in Lloyd's stand-alone cyber policies from March 2023	Evidence helps establish what is in scope of cover and prevents surprises at claim time
Retentions and deductibles	Set by insurer and negotiated	Stronger evidence may support negotiation of retention or sub-limit terms; outcome is insurer-specific
Underwriting confidence	Underwriters price uncertainty as well as expectation	Evidence packs narrow uncertainty; unanswered OT questions may be read cautiously
Risk questionnaires	Content varies widely across forms	Prepared, consistent answers reduce error and inconsistency across insurers and years
Evidence requirements	Larger risks may involve calls, surveys or scans	A ready evidence pack shortens the process and shows programme maturity
Renewal discussions	Renewal is where changes in controls are examined	Documented year-on-year improvement supports a narrative beyond the questionnaire
Risk remediation requirements	Insurers may set conditions or recommendations	A dated remediation register lets the operator propose credible timelines
Limits of coverage	Limits are bought against modelled scenarios	Financial quantification of residual OT exposure (Section 11) informs limit choice
Negotiation leverage	Depends on market cycle and insurer appetite	Leverage is greater in hard markets when capacity is scarce; it is smaller in a soft market such as 2026

EMERGING PRACTICE / HYPOTHESIS The strongest realistic outcome is not a discount but clarity: knowing which OT scenarios are covered, where the exclusions bite, and how much loss the operator retains. That clarity is worth having even when the market is soft and premiums are falling for everyone.

9. Sector-by-sector analysis

Sectors differ in OT footprint, loss scenarios, regulatory context and how insurers may treat them. The same underwriting treatment should not be assumed across sectors. Figure 7 combines the only documented sector-level likelihoods available with the author's directional view of exposure characteristics.

9.1 Manufacturing

Dimension	Analysis
OT exposure	PLCs, HMIs, engineering workstations, MES and historians; heterogeneous plants with long-lived equipment; increasing IT/OT integration and remote vendor support
Major cyber-loss scenarios	Plant shutdown from ransomware that reaches production or forces precautionary shutdown; data manipulation affecting quality; recovery of engineering workstations. JLR (2025) shows an IT-origin event halting production for weeks
Relevant IEC 62443 practices	Asset inventory; zone and conduit segmentation between corporate IT, DMZ and cells; remote-access control; backup of controller and engineering files; OT incident response
Evidence that could matter	Cell-level architecture, recovery-time evidence for critical lines, vendor access logs, tested restore of engineering data
Potential insurance implications	Business interruption is the dominant scenario; waiting periods, BI limits and contingent BI wording matter as much as price. Modelled manufacturing likelihood is 0.71% globally and 1.64% in North America. Shieldworkz identifies manufacturing as critical-risk in its advisory

9.2 Aerospace and defense

Dimension	Analysis
OT exposure	Test and production facilities, precision machining, controlled environments, sensitive design data, deep supplier tiers and government customer requirements
Major cyber-loss scenarios	Production stoppage; compromise of sensitive systems; supplier-originated compromise; state-actor targeting. The Shieldworkz advisory lists defense industrial among its critical-risk sectors
Relevant IEC 62443 practices	Zone and conduit design for production and test enclaves; supplier and integrator requirements; access control; monitoring. Defense-specific frameworks (for example NIST SP 800-171-based regimes in the US supply chain) commonly sit alongside, and mainly address information protection rather than plant OT
Evidence that could matter	Supplier assurance records, enclave architecture, monitoring, incident response with reporting obligations
Potential insurance implications	Not modelled initially. State-backed attack exclusions and government-contract obligations are likely to matter more than control credits. Treat pricing effects of IEC 62443 as unevidenced

9.3 Maritime

Dimension	Analysis
OT exposure	Vessel propulsion and power management, navigation and cargo systems, port interfaces, satellite and remote connectivity, shore-based operations
Major cyber-loss scenarios	Loss of navigation or propulsion integrity, cargo-system disruption, port delays, remote-access compromise, third-party service outage

Dimension	Analysis
Relevant IEC 62443 practices	Zones for shipboard OT, controlled remote access, supplier product requirements. IACS unified requirements on cyber resilience of ships (UR E26 and E27) apply to new ships contracted from 1 July 2024 [19]; their structure resembles IEC 62443 concepts, and mapping between them is the author's analysis, not an IACS statement
Evidence that could matter	Onboard architecture, remote-access records, supplier component evidence, class-society compliance
Potential insurance implications	Marine policies have long contained cyber-attack exclusions, with buy-back endorsements available in the market; wording varies and should be verified with the broker. Class compliance may be a stronger underwriting signal here than IEC 62443 labels

9.4 Utilities (power, transmission, distribution, water)

Dimension	Analysis
OT exposure	Generation and substation control, SCADA, distributed energy resources, water treatment control, distributed field assets, legacy protocols
Major cyber-loss scenarios	Loss of supply, manipulation of distributed assets, state-actor pre-positioning, ransomware in corporate systems affecting operations. The Shieldworkz advisory reports a December 2025 attack on Polish distributed energy sites
Relevant IEC 62443 practices	Zoning of control and DER environments; secure remote access; monitoring; incident response with regulator liaison; supplier requirements
Evidence that could matter	Regulatory compliance records (for example NERC CIP or NIS2 regimes where applicable), architecture, monitoring coverage, restoration exercises

9.5 Oil and gas / energy

Dimension	Analysis
OT exposure	Process control and safety instrumented systems, pipelines, refineries, upstream platforms, distributed remote sites and satellite links
Major cyber-loss scenarios	Precautionary or forced shutdown, safety system compromise (as with TRITON), pipeline disruption. Colonial Pipeline (2021) halted pipeline operations after an IT-side ransomware event
Relevant IEC 62443 practices	Segregation of safety and control zones; controlled remote access; asset inventory across distributed sites; OT incident response and recovery; supplier product security
Evidence that could matter	Safety-system isolation records, architecture, recovery plans, vendor access controls
Potential insurance implications	Property and casualty policies dominate energy risk; whether physical damage and BI from a cyber cause are covered depends on cyber exclusions and endorsements.

9.6 Pharmaceuticals and chemicals

Dimension	Analysis
OT exposure	Batch and continuous process control, validated systems, laboratory and quality systems, hazardous-process controls
Major cyber-loss scenarios	Production loss, loss of batch integrity, safety and environmental incidents, regulatory action. Merck's NotPetya experience shows both scale and coverage dispute risk
Relevant IEC 62443 practices	Zone design consistent with process safety; change control and system integrity; backup and re-validation planning; supplier and product security

Dimension	Analysis
Evidence that could matter	Validated-system inventory, recovery and re-validation time evidence, safety-system separation, regulatory compliance
Potential insurance implications	Modelled likelihood is highest among the sectors shown: For chemical manufacturing and 1.43% for pharmaceuticals Environmental liability and product-recall exposures may sit outside cyber cover

9.7 Transportation (rail, airports, logistics)

Dimension	Analysis
OT exposure	Rail signalling and control, airport baggage and building systems, logistics automation, third-party operational platforms
Major cyber-loss scenarios	Service disruption, safety-related shutdown, third-party platform outage affecting many operators. Shieldworkz has published analysis of European airport disruption (shieldworkz.com/reports)
Relevant IEC 62443 practices	Zone and conduit design; remote and supplier access; monitoring; in rail, CENELEC TS 50701 applies IEC 62443 concepts to railway systems
Evidence that could matter	Operational-continuity plans, supplier assurance, architecture, incident response and regulator engagement
Potential insurance implications	Government ownership, statutory regimes and concentration on shared third-party systems shape risk transfer more than security level evidence

10. OT cyber-insurance readiness framework

The framework helps a CISO prepare before approaching an insurer through the broker. It is the author's synthesis; no insurer has endorsed it. Figure 4 offers a maturity model for self-assessment and Figure 6 shows the evidence pack. Figure 5 illustrates the change in state that IEC 62443-aligned risk management aims to produce.

Figure 4 · OT cyber-insurance readiness maturity model

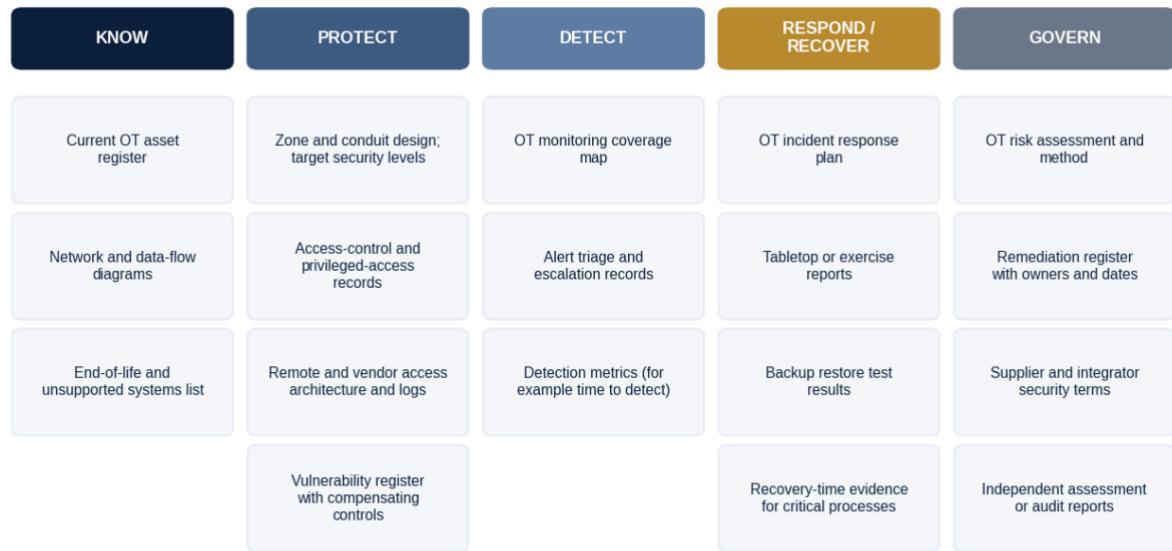
Author's framework for self-assessment; not an insurer, IEC or industry standard. Underwriting notes are hypotheses

	Level and name	What the operator can demonstrate	Likely underwriting conversation
5	Verified	Independent assurance or continuous telemetry supports claims; detection and recovery are measured; residual loss is quantified	Can discuss structure, limits and retentions with data (emerging practice)
4	Evidenced	Current asset register, architecture and zone documents, remote-access records, tested OT incident and recovery plans, KPIs	Evidence-backed submission; can challenge generic questionnaire scoring
3	Structured	OT risk assessment complete; zones and target security levels defined; policies documented; remediation register exists	Credible roadmap; gaps explained and dated
2	Aware	Partial asset inventory; informal segmentation; generic (IT) response plan; little OT-specific evidence	Narrative answers; limited negotiating leverage
1	Unassessed	No reliable OT inventory; IT questionnaire answers stand in for OT; OT questions answered by estimate or left blank	Unanswered OT questions may be read as risk signals by some underwriters [16]

Source: author's framework. Level descriptions are self-assessment aids; no insurer is known to score submissions against these levels. The 'unanswered questions' note reflects one vendor-reported underwriting methodology [16] and should not be generalised.

Figure 6 · OT operator evidence pack for cyber-insurance underwriting

Artefacts an operator can assemble before renewal; content should be shared under confidentiality terms



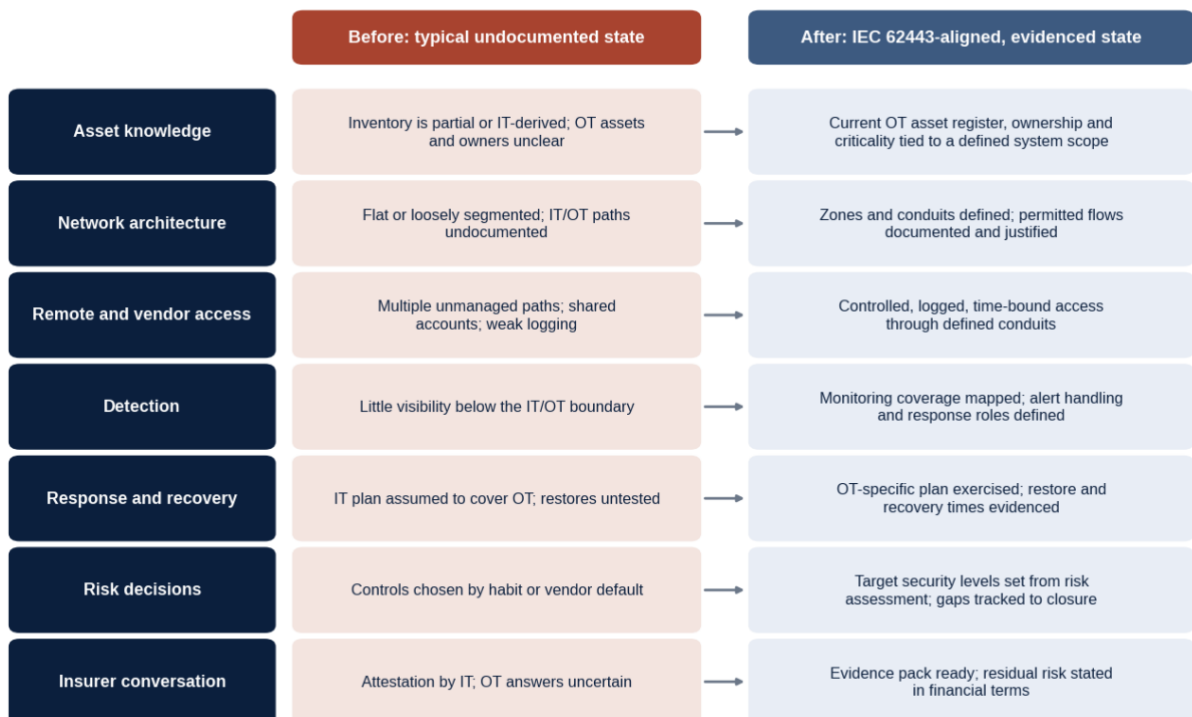
Using the pack:

Lead with scope (which sites and systems), date every artefact, and state what is not yet in place. Evidence that is current and inspectable is more useful than a certificate alone; a certificate or assessment report supports the pack but does not replace it.

Source: author's synthesis; artefact categories align with information requests reported by practitioners in [2] and [16], and with IEC 62443 programme and risk-assessment practices.

Figure 5 · Before and after IEC 62443-aligned risk management

Illustrative characterisation of typical operator states; outcomes depend on execution and are not guaranteed



Source: author's synthesis of IEC 62443 practice areas and insurer information requests reported in [2] and [16]. Not a claim that any specific insurer will change terms.

Readiness categories: what insurers may want and what to demonstrate

Category	What insurers may want to understand	What the operator should demonstrate	Typical evidence
1. OT asset visibility	What OT assets exist, where, who owns them, how critical they are	A current register covering all in-scope sites, refreshed on a stated cycle	Register, discovery scan or passive-monitoring inventory, ownership list
2. OT risk assessment	Whether consequences and threats have been assessed for OT specifically	A method-based assessment with scenarios and consequences, not a generic IT risk register	Risk assessment report, scenario list, approval record
3. Zones and conduits	How IT and OT are separated and what can traverse	Zone and conduit register and justified rule set	Architecture diagrams, firewall rule reviews, conduit inventory
4. Security levels	Whether protection is matched to consequence	Target SL per zone and a defined gap to achieved	SL-T register, SL-A assessment, gap list
5. Identity and access management	Who and what can change OT, with what accountability	Individual accounts, MFA where feasible, privileged access controlled	IAM records, privileged-access logs, review evidence
6. Remote and vendor access	How third parties reach OT	Single controlled path with approval, logging and session recording	Architecture, vendor list, session logs
7. Vulnerability management	How OT weakness is found and treated	Prioritised register with decisions, including where patching is not possible	Vulnerability register, patch or compensating-control decisions
8. Network monitoring	Visibility into OT traffic and anomalies	Monitoring coverage of critical zones with defined tuning	Coverage map, sensor placement, alert records
9. Incident detection	Whether OT events are recognised and escalated	Defined detection use cases and escalation	Use-case list, alert handling records, metrics
10. Incident response	Whether an exercised OT plan exists	OT-specific plan with roles, safety interfaces and vendor contacts	Plan, exercise reports, lessons-learned log
11. Backup and recovery	Whether OT configurations can be restored	Offline, tested backups of controller and engineering data	Backup scope, restore test records, recovery times
12. Business continuity	Whether operations can continue or restart	Manual-operation and restart procedures for critical processes	BCP for OT, manual-mode drills, dependency map
13. Third-party risk	How supplier risk is managed	Supplier tiers, contractual security clauses and assurance	Supplier register, contract clauses, assurance records
14. Governance	Whether the programme has ownership and continuity	Named accountable executive, policies and metrics reviewed	Policy set, RACI, KPI reports, management review minutes
15. Regulatory compliance	Which laws and sector rules apply	Applicability map and evidence of compliance	Compliance register, audit results
16. Security evidence	Whether claims can be verified	A dated evidence pack organised by pillar (Figure 6)	Evidence index, version history, owner sign-off

Common weaknesses, remediation and potential underwriting relevance

Category	Common weaknesses	Recommended remediation	Potential underwriting relevance
1. OT asset visibility	Spreadsheet from years ago; IT tools blind to controllers; no criticality	Passive discovery plus quarterly reconciliation; assign owners	Foundation for every other answer; reduces uncertainty
2. OT risk assessment	IT risk method reused; no consequence analysis; stale	Adopt a 62443-3-2-style assessment; link scenarios to loss estimates	Ties controls to loss scenarios; supports limit selection
3. Zones and conduits	Flat networks; undocumented paths; stale rules	Segment by consequence; review rules; document exceptions	Severity and lateral-movement exposure
4. Security levels	SLs asserted without method; single level everywhere	Derive SL-T from risk assessment; track gaps	Shows risk-based targeting rather than blanket claims

Category	Common weaknesses	Recommended remediation	Potential underwriting relevance
5. Identity and access management	Shared and default credentials; no review cycle	Individual accounts; PAM for engineering access; periodic review	Credential compromise exposure
6. Remote and vendor access	Multiple unmanaged vendor VPNs and modems; no logging	Consolidate access; time-bound approvals; enforce MFA	Third-party attack surface
7. Vulnerability management	Patching ignored due to uptime fear; no register	Risk-based process with compensating controls	Remediation discipline; legacy explanation
8. Network monitoring	IT monitoring stops at the boundary	Passive OT monitoring for critical zones	Detection capability and dwell time
9. Incident detection	No OT-specific use cases; alerts unowned	Define use cases; assign 24x7 or on-call ownership	Time to detect; potential loss window
10. Incident response	IT plan assumed to apply; never exercised with operations	OT playbooks; annual joint tabletop	Business-interruption duration
11. Backup and recovery	Backups exist but never restored; single copy	Offline copies; scheduled restore tests	Recovery time; ransomware resilience
12. Business continuity	Dependence on IT systems unrecognised	Map dependencies; rehearse manual and restart modes	BI severity and duration
13. Third-party risk	No OT security terms in integrator contracts	Standard clauses aligned to 2-4 and 4-1 topics	Supply-chain exposure
14. Governance	Security owned by a project; IT and OT teams split	Establish OT security governance forum and metrics	Confidence that controls persist
15. Regulatory compliance	Requirements known only to legal team	Consolidated obligations map linked to controls	Regulatory loss exposure
16. Security evidence	Evidence scattered; no version or date	Central repository, named owner, refresh cadence	Underwriting confidence and speed

11. Quantifying the business case

A defensible business case connects controls to expected loss, residual exposure and the insurance structure. It should not be built on an assumed premium discount. The illustrative model below uses one documented likelihood and one documented control effect, and labels everything else as an assumption. Replace the assumptions with the organisation's own data.

Model structure

Baseline exposure, then probability of a disruptive incident, then operational loss, then expected annual loss, then reduction from controls, then residual exposure, then insurance structure and uninsured tail.

Inputs and their status

Input	Value used	Status
Revenue and contribution margin	USD 1.0bn; 30% (USD 0.82M contribution per outage day)	Assumption
Annual likelihood of OT-involved breach	1.64% (manufacturing, North America)	Documented sector-level model output likelihood rises with revenue, so a firm of this size may sit above average
Moderate event	12 full-outage-equivalent days plus USD 2.5M response and recovery: USD 12.4M	Assumption
Severe event	45 days plus USD 8.0M response and recovery: USD 45.0M	Assumption; duration chosen to be comparable in order of magnitude to published multi-week manufacturing outages
Event mix	80% moderate, 20% severe: expected loss per event USD 18.9M	Assumption
Control effect	19.38% (manufacturing incident response planning) with 10% and 30% bounds	19.38% documented; bounds are the author's; report states effects are not additive
Insurance structure	USD 1M retention, USD 25M limit, full response	Assumption; ignores exclusions, waiting periods and sub-limits
Likelihood stress	3 times sector average: 4.92%	Author's stress test

Results

Case	Expected annual loss (USD M)	Residual after 19.38% (USD M)	Range at 10% to 30% (USD M)
Sector-average likelihood (1.64%)	0.31	0.25	0.22 to 0.28
3 times stress (4.92%)	0.93	0.75	0.65 to 0.84

What the model does and does not show

- **Expected loss is small relative to the tail.** At average base rates, the annual expected-loss reduction from controls is about USD 0.06M for this hypothetical operator. That is far smaller than typical programme costs, so the case for OT security spend cannot rest on expected-loss savings or a premium discount alone.

-
- **The tail is the material exposure.** The severe event exceeds the assumed USD 25M limit by about USD 19M. Limit adequacy, retentions, exclusions and waiting periods determine the uninsured share; this is where evidence, structure and coverage clarity matter.
 - **Non-financial drivers are not in the model.** Safety, regulatory, customer and licence-to-operate consequences, and the value of insurability itself, sit outside the arithmetic.
 - **Premium is not modelled.** Insurers price with their own loss history, exposure data, reinsurance cost and appetite. The model has no premium output because no public rating formula exists to support one.

HOW TO USE

Substitute the operator's own revenue, margin, plant-level outage costs and scenario likelihoods. Use the result to answer three board questions: what could we lose, how much would insurance pay under our actual wording, and which controls reduce the uninsured tail. Broker modelling and insurer views should replace the assumptions before any decision.

12. What CISOs should take to the board

1. **OT security maturity matters to insurance mainly through evidence.** Insurers price uncertainty as well as expected loss. Dated, scoped evidence narrows it; assertions do not.
2. **IEC 62443 can demonstrate structure.** It gives a recognised vocabulary and method for asset identification, zoning, target security levels, governance and supplier expectations, and produces artefacts an underwriter can inspect.
3. **It cannot demonstrate, by itself, that controls work today.** A certificate or assessment has a scope and date and does not prove current configuration, coverage of all sites or tested recovery.
4. **Certification alone is insufficient.** Its scope varies by scheme and object certified, and no public evidence shows insurers treating it as a defined pricing input.
5. **Premium reduction is not a reliable benefit to plan on.** The market cycle dominated pricing through mid-2026, and public research has found premiums driven mainly by exposure measures.
6. **The indirect case is credible.** Modelled claims data associate incident response planning, defensible architecture and monitoring with roughly 16 to 19% average modelled risk reduction, and higher in electric power. The effects are not additive and are not specific to IEC 62443.
7. **Prepare for underwriting as for an audit.** Build the evidence pack (Figure 6), agree scope with the broker, and state gaps with dates rather than leaving them unanswered.
8. **Quantify residual OT risk in money.** Model severe scenarios against actual limits, retentions, exclusions and waiting periods. In the illustrative model the uninsured tail, not expected loss, is the material figure.
9. **Test coverage, not just controls.** Ask the broker where cyber and property wording leave OT-induced physical damage and business interruption, and how state-backed attack exclusions would apply.
10. **Connect investment to exposure, not to a discount.** Frame OT security spend as reducing tail loss and uninsured exposure, protecting safety and licence to operate, and improving insurability; treat any premium benefit as upside.
11. **Keep the claim honest.** State to the board what is established, what is plausible, what is emerging and what depends on the insurer.

13. 90-day OT cyber-insurance readiness roadmap

The roadmap assumes a multi-site industrial operator starting from partial visibility. Adjust durations to scale. Owners are role titles; KPIs are examples to be calibrated.

Days 0 to 30: establish visibility and identify evidence gaps

Deliverable	Owner	Evidence	KPI	Dependencies
Scope and sites agreed with broker	CISO, risk manager	Scope statement, list of sites and systems	Scope signed off	Broker engagement; policy wording obtained
OT asset inventory baseline	OT security lead, plant engineers	Asset register with criticality and owner	% of critical assets inventoried	Access to plants; discovery tooling
Architecture and remote-access review	OT security lead, network team	Diagrams; list of all remote paths and vendors	Number of unmanaged paths identified	Vendor cooperation
Baseline IEC 62443 assessment	OT security lead, assessor	Gap register with target and achieved levels	Gaps listed and rated	Inventory and architecture inputs
Coverage review	Risk manager, broker	Map of cyber, property and BI wording against OT scenarios	Scenarios mapped to policies	Policy documents

Residual risks at day 30: incomplete inventory at low-priority sites; gaps found but not yet funded.

Days 31 to 60: address priority IEC 62443 security gaps

Deliverable	Owner	Evidence	KPI	Dependencies
Remove or control unmanaged remote paths	OT security lead, vendor managers	Access architecture, MFA and logging records	Unmanaged paths closed	Vendor change windows
Segmentation fixes at critical zones	Network team, plant engineers	Updated rule sets and zone register	Critical zones with reviewed conduits	Maintenance windows
OT incident response plan and tabletop	CISO, plant operations	Plan, exercise report, actions	Exercise completed; actions tracked	Operations and safety participation
Backup and restore test for critical controllers	OT engineering	Restore test record, recovery time	Restore success and time	Offline storage; test window
Remediation register with owners and dates	OT security lead	Register with funding status	% of priority gaps assigned and funded	Budget approval

Residual risks at day 60: legacy systems that cannot be patched or replaced quickly; monitoring coverage not yet in place; plant resistance to change during production.

Days 61 to 90: build the insurance underwriting evidence package

Deliverable	Owner	Evidence	KPI	Dependencies
OT monitoring coverage for critical zones	OT security lead, SOC	Coverage map and alert handling evidence	% critical zones monitored	Sensor deployment
Evidence pack assembled and dated	CISO	Pack indexed by pillar (Figure 6)	Pack complete; owner sign-off	Prior phases
Residual exposure quantification	Risk manager, finance, broker	Scenario loss model against actual insurance structure	Scenarios with uninsured share stated	Plant BI estimates; broker input
Underwriting submission and meeting plan	CISO, broker	Draft narrative, gap list, remediation dates	Submission ready before renewal	Renewal timetable
Governance cadence	CISO	Quarterly evidence refresh schedule	Refresh cadence in place	Management approval

Consolidated residual risks

- Insurer response is outside the operator's control; the pack improves the conversation but does not guarantee changes in terms or price.
- Evidence ages: a pack not refreshed loses value within a renewal cycle.
- Gaps in legacy environments will persist beyond 90 days; the goal is a documented, funded plan.
- Operations may resist change in production environments; joint ownership with plant leadership is a dependency.

14. Assessment tooling: OThello from Shieldworkz

The preceding analysis concluded that the operator-controlled value lies in current, inspectable evidence of OT posture. A practical obstacle is time and effort: building an IEC 62443 gap picture manually across sites can take months. This section describes one technology option, OThello from Shieldworkz, the publisher of this paper. The interest is disclosed; the paper's conclusions do not depend on this section.

PROPOSITION | As stated by Shieldworkz

OThello can conduct an IEC 62443 assessment in 24 to 48 hours. This describes the speed of establishing a current posture. It does not describe remediation or certification.

What OThello is positioned to do

- **Assess IEC 62443 posture** against relevant requirements and produce a baseline view for a defined scope.
- **Identify security gaps** and map findings to IEC 62443 requirements.
- **Structure assessment evidence** so that findings, sources and dates are organised for review.
- **Establish security levels where applicable** by comparing target and achieved levels.
- **Identify remediation priorities** so that limited engineering effort goes to the gaps that matter.
- **Create an assessment trail** that shows what was assessed, when and on what basis.
- **Accelerate preparation for internal or external review**, including discussion with auditors, brokers and insurers.
- **Improve evidence available to security and risk stakeholders**, including inputs for the evidence pack in Figure 6.

What it is not

Distinction	Meaning
Assessment speed is not remediation speed	A posture picture in 24 to 48 hours does not close the gaps it finds. Remediation depends on engineering change, maintenance windows, procurement and plant operations.
Assessment speed is not compliance certification	Rapid assessment does not make an organisation IEC 62443 compliant, and it is not an independent certification by a recognised body.
A tool is not governance	OThello does not substitute for security governance, engineering remediation, independent assurance or the broader IEC 62443 framework.
An assessment is not an insurance outcome	No insurer is known to credit a specific tool or report with a defined premium effect. Its value is the evidence and clarity it creates.

Where it fits in the roadmap

In the 90-day roadmap, a rapid assessment supports days 0 to 30 by establishing the baseline gap register and target-versus-achieved view, and later supports refresh of evidence for the pack. The value proposition is the ability to rapidly establish current posture, identify gaps and create an actionable, evidence-backed remediation path. Independent verification of the results, especially before they are shown to an insurer or regulator, remains a separate step.

15. Conclusion

THE QUESTION

Can IEC 62443 compliance reduce OT cyber-insurance premiums?

It can plausibly contribute to better insurance outcomes, but public evidence does not show that compliance or certification reduces premiums by a defined amount. The defensible answer separates four levels of support:

Level	Statement
Demonstrably supported	Controls organised by IEC 62443 (architecture, access, monitoring, response) correspond to controls associated with lower modelled loss in claims-based research. OT losses can be large, mostly indirect and partly uninsured. Market cycle strongly influences premiums
Logically plausible	Operators with current, inspectable OT evidence present a narrower and more verifiable risk than those without, and are better placed to negotiate scope, terms and limits
Emerging	Some insurers, brokers and vendors report growing interest in OT security maturity and framework adherence, with OT-specific questionnaires and tools appearing
Dependent on insurer-specific underwriting	Whether any evidence changes price, retention, limits or terms for a given operator

The central message follows. **IEC 62443 should be viewed not merely as a compliance exercise, but as a structured method for identifying, managing and demonstrating OT cyber risk.** Its return in insurance terms comes first through insurability, coverage clarity and reduced uninsured exposure, and possibly through price where an insurer can see and credit the evidence. The claim that compliance automatically produces a specific insurance discount is not supported and should not be made.

Three developments would change this assessment: an insurer or rating body publishing an OT rating variable tied to IEC 62443, empirical studies of OT claims with control-level data, and a hardening market in which underwriters differentiate more strongly. Operators who have already built the evidence pack will be positioned to benefit under any of them.

References

Numbers in brackets refer to this list. Vendor and publisher sources are labelled and used only for what they can establish.

Sources
Marsh, Global Insurance Market Index, Q2 2026, 23 July 2026.
Romanosky, S., Ablon, L., Kuehn, A., Jones, T., "Content analysis of cyber insurance policies: how do carriers price cyber risk?", Journal of Cybersecurity 5(1), 2019.
Woods, D., Agrafiotis, I., Nurse, J., Creese, S., "Mapping the coverage of security controls in cyber insurance proposal forms", Journal of Internet Services and Applications 8, 2017.
Skeoch, H. and Pym, D., "Pricing cyber-insurance for systems via maturity models", arXiv, 2023 (conceptual proposal; not used for quantitative claims).
Cyber Monitoring Centre, statement on the Jaguar Land Rover cyber event, 22 October 2025.
Cybersecurity Dive, reporting on the Merck and insurers NotPetya coverage settlement, January 2024.
Norsk Hydro quarterly disclosures as reported by Threatpost and CyberScoop (October 2019) and Reinsurance News (February 2020).
Security Magazine, reporting on NotPetya costs to A.P. Moller-Maersk, January 2022.
Lloyd's Market Bulletins Y5381 (August 2022) and Y5433 (May 2024) on state-backed cyber-attack exclusions; Clifford Chance analysis, September 2023.
Munich Re, Cyber Insurance: Risks and Trends 2026.
TXOne Networks, "OT Cybersecurity Insurance: Present Landscape and Future Outlook", 15 May 2025 (vendor commentary).
Smart Industry, trade press reporting on OT insurance requirements, December 2025.
DeNexus, "OT Underwriting Evidence Starts with the Right Questions", 17 June 2026, and related product announcements (vendor).
Shieldworkz, "Why IEC 62443 Is the Leading OT Cybersecurity Standard", 15 July 2026 (publisher's article).
Shieldworkz, H1 2026 OT Threat Advisory, 28 May 2026 (TLP:AMBER).
International Association of Classification Societies, Unified Requirements E26 and E27 on cyber resilience of ships and of on-board systems and equipment.
IEC and ISA public documentation of the IEC/ISA 62443 series; ISASecure and IECCE certification scheme descriptions; secondary summaries of part editions, including the 2024 revision of 62443-2-1. Primary standards texts should be consulted for normative wording.
Shieldworkz, OThello product information, shieldworkz.com.
Shieldworkz, "A deep dive into IEC 62443-3-3 controls for OT operators", 24 November 2025.

About Shieldworkz

Shieldworkz is a specialist OT/ICS cybersecurity firm with an NDR solution and AI-based tools for securing SCADA, PLCs and Cyber Physical Systems. We serve critical infrastructure operators, industrial organisations, and government entities across the energy, oil and gas, manufacturing, utilities, transport, and defence sectors.

Our service areas include OT security assessments (powered by OThello Assess with sub-24-hour assessment cycles), NIS2 and IEC 62443 compliance programmes, OT threat intelligence advisories, OT SOC design and implementation, and regulatory readiness engagements for NCA (Saudi OTCC/ECC), NERC CIP, SOCI, and Singapore Cybersecurity Act obligations.

Reach out to us at info@shieldworkz.com for a briefing

NDR Solution: shieldworkz.com/products/ot-security-platform | **Media Scan:** shieldworkz.com/products/ot-security- | **Othello Assess:** shieldworkz.com/othello/assess | **Patch Management:** shieldworkz.com/products/patch-management-solution | **Regulatory Playbooks:** shieldworkz.com/regulatory-playbooks | **Remediation Guides:** shieldworkz.com/remediation-guides | **Reports:** shieldworkz.com/reports

About Shieldworkz



ISOC and Honeypot Locations

Honeypot Locations



Security Operations Center



Shieldworkz is a global OT security company founded by top industry experts to protect critical infrastructure using proprietary technology and a leading consulting platform, we partner with businesses to secure assets, networks, and programs across industries. Our services are tailored to each client's cyber risks and backed by the world's largest OT and IoT threat intelligence facility and a global research team.

Secure Your Industrial Future

Talk to us today!



From OT security assessments covering NIS2, IEC 62443, NERC CIP and other regional requirements to an OT security platform, Shieldworkz covers all compliance and industrial cybersecurity enhancement needs. Talk to us to learn how you can enhance your security posture in 7 easy steps.

Contact Us



GERMANY

- 📍 Fritz-Schäffer-Street 1,
4th floor
Bonn, 53113, Germany
- ☎ +49 (0) 228 / 929 39210
- ✉ europe@shieldworkz.com

CANADA

- 📍 396 Old Colony Road
Richmond Hill,
ON L4E 5A5 Canada
- ☎ +1 (437) 223-7770
- ✉ americas@shieldworkz.com

UAE

- 📍 Tenth floor,
Abu Dhabi,
United Arab Emirates,
FAB Business Center
- ☎ +971 56 660 5200
- ✉ middleeast@shieldworkz.com

INDIA

- 📍 Gopalan Signature Tower,
No 6, 2nd Floor, Old Madras
Road, Benniganahalli
Bengaluru,
Karnataka 560093
- ☎ +91 9059620557
- ✉ apac@shieldworkz.com

