The Encryption of Operational Technology: A Protocol Landscape

Bruno Salmazo

Liscere

July 2026 · Liscere Briefing · LB-2026-02 · v1

Executive Summary

The preceding Liscere Technical Report [1] established, in hardware, that strong transport encryption changes the observation vantage available to a contextual evaluator of industrial control actions, not the evaluation core itself. It named, as its first research front, an empirical question: how much of operational technology is encrypted, by what mechanism, and with what trajectory. This briefing answers that question from the published evidence.

We survey the dominant OT protocol classes: the field-level real-time protocols that carry the majority of new factory-automation nodes, the supervisory layer around OPC UA, the energy-sector telecontrol and substation stack, vendor management channels, and the IIoT broker layer. For each class we document the standardised security mechanism, its treatment of confidentiality, and the measured state of adoption, labelling every claim by the strength of its evidence.

Three findings organise the landscape. First, encryption capability and encryption activation are different quantities, and the gap between them is large, persistent, and measured: internet-wide scans place TLS adoption on industrial protocols in single-digit percentages, and the misconfiguration pattern documented for OPC UA in 2020 is intact in 2025. Second, where OT security standards do land, they deliberately prioritise integrity and authenticity over confidentiality for real-time control data; in the substation domain this preference is codified, with the applicable standard stipulating that time-critical protection traffic is not to be encrypted. Third, encryption arrives stratified by functional plane: vendor management channels first, vertical supervisory links slowly, the real-time protection plane last or never. The consequence for observation is stated as a vantage matrix: the case of an opaque channel with no natural point of legitimate access is confined to a single protocol class, and even there, secondary evidence sources exist.

Keywords: operational technology, industrial protocols, encryption adoption, OPC UA, IEC 62351, TLS, passive monitoring, observation vantage.

1. Introduction and scope

The question this briefing addresses was posed, but not answered, by the hardware work that precedes it. LTR-2026-04 [1] characterised one encrypted control channel, the Web API of a Siemens S7-1200 G2, and isolated an architectural fact: passive observation of payload is physically impossible under strong transport encryption, so what an encrypted channel changes is the vantage from which evidence is drawn, not the logic that evaluates it. The practical weight of that fact depends on an empirical variable the report deliberately left open: how much of operational technology is, or is becoming, encrypted. A vantage problem that covers the whole field demands a different response from one confined to a narrow class of channels.

This briefing sizes the variable. It is a landscape study, not an experiment: its method is the systematic reading of measurement literature, standards documents, and industry sources, and its contribution is the organisation of that evidence into a form that supports architectural reasoning. It also discharges a

commitment made in the preceding report, whose related-work positioning on encrypted OT protocols was deferred to this study.

Two disciplines govern the writing. The first is evidence labelling. Sources in this domain range from peer-reviewed internet-wide measurement to vendor marketing, and conclusions built without distinguishing them are built on sand. Every load-bearing claim in this briefing carries one of four labels: measured (peer-reviewed measurement studies and public scans with published methodology), reported (surveys, standards bodies, government agencies), vendor-claimed (vendor and foundation publications, manufacturer documentation), and inferred (our own extrapolation, always marked). The second discipline is the separation of what is observed from what it means for any particular system. This briefing describes the field; it selects no architecture and evaluates no product.

One scope caveat applies throughout and is repeated where it bites. The strongest quantitative evidence on security adoption comes from internet-wide scans, which by construction measure the internet-exposed population. Internal OT networks cannot be scanned from outside, and no comparable measurement of the internal installed base exists. Where we reason from exposed populations to internal practice, the step is labelled as inference.

2. The protocol classes and their security mechanisms

Operational technology does not run on one protocol, and its encryption story cannot be told as one story. We organise the field into five classes, chosen because each has a distinct security mechanism and a distinct adoption dynamic.

2.1 Field-level real-time protocols

PROFINET, EtherNet/IP, and EtherCAT together account for 67% of newly installed factory-automation nodes in the most recent industry analysis, at 27%, 23%, and 17% respectively, with Industrial Ethernet as a whole at 76% of new nodes and traditional fieldbuses declining to 17% [2] (vendor-claimed; this is the only recurring quantitative source on node shares and is treated as directional rather than precise).

PROFINET is introducing protocol-level security in three incremental classes [3]. Security Class 1 is hardening: signed device-description (GSD) files, read-only device discovery, SNMPv3. It has moved to concrete implementation, with the standards body operating signing infrastructure and vendor engineering tools already covering it. Classes 2 and 3 have their cryptographic elements defined in recent specifications, with device development beginning; they are not yet products in the field. The design detail that matters for observation is explicit in the standard's own material: Class 2 protects the integrity and authenticity of cyclic IO data but does not encrypt it, on the stated grounds that IO data is not routable; only Class 3 encrypts cyclic data, and the standards body frames Class 3 as applicable where trade secrets could be inferred from the data itself (reported).

CIP Security, the security extension for EtherNet/IP, uses TLS and DTLS transports with X.509 certificates or pre-shared keys, and makes message encryption an optional, negotiated attribute on top of mandatory integrity [4]. The publisher's own deployment guidance is selective rather than blanket: CIP Security is positioned for the zones where risk is most critical, within a defence-in-depth architecture, with the EU Cyber Resilience Act and IEC 62443 cited as the drivers for shipping the capability (vendor-claimed).

EtherCAT takes the position furthest from channel encryption. The EtherCAT Technology Group's security model rests on the segment architecture itself, since EtherCAT segments are not IP-routable, combined with controller-level access control; the group's public position is that this meets IEC 62443 and Cyber Resilience Act requirements for almost all common applications without protocol changes [5]. Its whitepaper states the rationale plainly: only in very few applications do users additionally require encryption of process and parameter data, because the damage that could result from data disclosure is usually minimal. For the exceptional cases, the group is specifying an optional, backward-compatible

authenticated encryption extension, notable for being designed as quantum-secure from the outset (vendor-claimed).

2.2 The supervisory layer: OPC UA

OPC UA, standardised as IEC 62541, is the dominant vendor-neutral protocol of the supervisory and vertical-integration layer, connecting controllers to SCADA, MES, historians, and cloud systems, with over a thousand member companies behind its foundation and several hundred companion information models [6] (vendor-claimed). It does not appear in field-level node counts because it is not, today, a field protocol; the OPC UA FX extension aims to change that, with specifications complete, certification launched, and first certified devices expected from 2026 (vendor-claimed). The layer OPC UA already occupies is the one that carries operator and HMI setpoint writes, which makes its security model consequential now, not only in the FX future.

That security model is negotiated per endpoint as a combination of a Security Mode and a Security Policy [7]. The three modes are None, Sign, and SignAndEncrypt. The middle mode deserves emphasis, because it is invisible in a binary clear-versus-encrypted framing: under Sign, messages carry cryptographic signatures but the payload travels in clear. Policies name the cipher suites; Basic128Rsa15 and Basic256 are deprecated, Basic256Sha256 is the recommended minimum, and elliptic-curve policies exist in the current specification but are described by implementers as experimental in practice (reported, vendor-claimed).

For publish-subscribe communication, Part 14 of the specification defines a different model again: group-based message security, in which a Security Key Service distributes symmetric group keys of limited lifetime to publishers and subscribers over conventional secure connections, and messages are then signed and, optionally, encrypted end to end across any transport [8] (reported). The observation consequence is developed in Section 5.

2.3 The energy sector: telecontrol and substations

The energy sector has the most mature protocol-security standardisation in OT, centred on the IEC 62351 series, which now spans more than twenty documents [9]. Its structure is a study in deliberate differentiation by traffic class.

For the telecontrol protocols, IEC 60870-5-104 and DNP3, two independent retrofit paths exist. IEC 62351-3 wraps the unchanged protocol in TLS with mutual certificate authentication, on the model of HTTPS. IEC 62351-5, and DNP3's native Secure Authentication built on it (SAv5 in IEEE 1815-2012, with a successor version since), changes the protocol instead, adding challenge-response authentication of critical operations inside the protocol itself; the payload remains readable, the port is unchanged, and communication degrades gracefully to the unauthenticated protocol for peers that do not support it (reported). The complete SAv5 protocol has received formal security analysis, which identified weaknesses in its composition [10] (measured). Practitioner reporting from utility deployment describes DNP3 Secure Authentication field adoption as light, with the interoperability burden falling on end users [11] (reported).

Within the substation, IEC 61850 splits sharply by traffic class. Its client-server profile, MMS, receives full TLS under IEC 62351-3 and -4, with the 2023 edition elevating the TLS part from technical specification to full international standard; the latency cost is deemed acceptable for monitoring and control. Its real-time protection traffic, GOOSE and Sampled Values, with delivery requirements in the low milliseconds, receives message authentication codes for integrity, authenticity, and replay protection under IEC 62351-6, and the series' own framework part stipulates that encryption algorithms are not to be applied to this traffic, on the grounds that encryption processing on resource-limited protection devices is incompatible with the delivery requirement [12] (measured, reported). For the routable variants, authenticity and integrity are mandatory and confidentiality is explicitly optional. Practice sits below even this: industry reporting

indicates that many utilities operate GOOSE without the authentication extension, relying on network isolation (vendor-claimed).

2.4 Vendor management channels

The channels through which engineering stations and HMIs manage controllers form their own class, and it is the fastest-moving one. The case measured in hardware in this series is the Siemens S7-1200 G2 Web API, JSON-RPC over HTTPS with TLS 1.3, session tokens, and per-user permissions [1] (measured). The same vendor's native engineering and HMI channel followed the same trajectory: its legacy protection rested on hardcoded global private keys, whose extraction was demonstrated publicly with the consequence, among others, that passively captured traffic could be decrypted [13] (measured); the remediation, from TIA Portal V17 with corresponding controller firmware, is genuinely TLS-based communication with per-device certificates, alongside a legacy and mixed mode retained for compatibility [14] (vendor-claimed). The general pattern, of which this is the documented instance, is that modern controllers ship HTTPS management interfaces with TLS by default and no clear mode; we state the cross-vendor generalisation as inference rather than measurement.

2.5 The IIoT broker layer

MQTT is the publish-subscribe backbone of edge-to-cloud industrial telemetry, and Sparkplug B standardises its topic namespace, payload structure, and state management for industrial use [15]. The layer is not control-free: the specification defines command messages for writing to nodes and devices, and unified-namespace architectures increasingly route setpoint changes through the broker (reported). Transport security here is IT-heritage TLS, positioned by the ecosystem as required.

3. Encryption in practice: capability against activation

The mechanisms of Section 2 describe what the field can do. The measurement literature describes what it does, and the two diverge widely and persistently.

The broadest single measurement is an internet-wide assessment of ten industrial protocols in their clear and TLS variants, covering the complete IPv4 address space [16] (measured). Its headline is stark: TLS-secured industrial deployments are barely noticeable in the wild. Overall TLS adoption stood at 6.5% of hosts, with a telling split between protocol generations: natively TLS-capable modern protocols reached 7.2%, while the retrofitted secure variants of traditional protocols, Modbus/TCP Security among them, stood at 0.4%. Close to a million hosts were found communicating insecurely, and of the hosts that did use TLS, 42% still showed configuration deficits.

OPC UA, as the protocol designed with security from the start, is the sharpest test of the capability-activation gap, and it has now been measured twice, five years apart. The 2020 internet-wide study found problematic security configurations on 92% of reachable deployments: missing access control on 24% of hosts, security disabled outright on 24%, deprecated cryptographic primitives on 25%, and hundreds of devices across networks sharing a single certificate [17] (measured). A commercial scan spanning June 2024 to June 2025 found the pattern intact: of 14,220 exposed OPC UA devices across 99 countries, 51.7% permitted anonymous interaction, and 80.3% of those reporting their supported modes offered the unencrypted None mode [18] (measured, with commercial methodology). Complementing the deployment scans, a systematic analysis of 48 publicly available OPC UA products and libraries found security issues in 38 of them, including seven with no support for the protocol's security features at all [19] (measured). The consistent reading across all three is that the deficits are not exotic: they are the ordinary condition of deployed OPC UA.

The same gap recurs wherever it can be measured. Modbus/TCP Security has existed since 2018, wrapping the unchanged protocol in TLS on a dedicated port with mutual certificate authentication and role-based

access control carried in a certificate extension [20] (reported); its measured presence is the 0.4% figure above. The one vertical with a regulatory driver is distributed energy resources, where the SunSpec profile mandates the TLS variant in the IEEE 1547 interconnection context [21] (reported). MQTT, whose ecosystem positions TLS as required, showed the 7.2% modern-protocol adoption figure in the same 2022 measurement, and recent assessments report tens of thousands of publicly reachable brokers accepting connections without authentication (measured).

Two qualifications keep this section honest. The first is the exposure caveat stated in Section 1: every figure above describes the internet-exposed population. It is plausible that internal deployments activate security even less often, since the assumption of a trusted internal network is precisely the reason operators give for leaving security off; but that is inference, not measurement. The second is that regulation is now pushing on the capability side of the gap: the Cyber Resilience Act and IEC 62443 are cited across the standards bodies of Section 2 as the reason security features are being specified and shipped. Shipping is not activation. The OPC UA record, secure by design and 92% deficient in deployment, is the measured warning against conflating them.

4. The deliberate preference for integrity over confidentiality

If Section 3 described a gap between intention and practice, this section describes something different: an intention. Across the standards bodies of Section 2, where security for real-time control data is specified at all, it is specified as integrity and authenticity, with confidentiality treated as an exception, an option, or an explicit exclusion.

The instances line up. OPC UA defines Sign as a first-class mode, authenticated but readable. PROFINET Security Class 2 protects cyclic IO data against modification but leaves it readable by design, with the standards body's stated reasoning that the data is not routable and its confidentiality unnecessary in the common case. CIP Security makes encryption an optional negotiated attribute above mandatory integrity, and its publisher recommends deploying it selectively. The EtherCAT Technology Group states that the damage from disclosure of process data is usually minimal and specifies encryption only as an exceptional-case extension. And the substation domain codifies the preference outright: IEC 62351 mandates message authentication for GOOSE and Sampled Values and stipulates that encryption is not to be applied to them, because the delivery requirement of protection traffic does not admit it.

The engineering reasons are consistent and sound: latency budgets measured in milliseconds, constrained compute on field devices, and the absence, for most IO data, of any secrecy requirement. The observation consequence, however, is rarely stated, and it is the pivot of this briefing: a binary framing of clear versus encrypted channels misses the largest category that OT security standardisation is actually building. Signed-but-readable is not a transitional state on the way to encryption. In the substation it is the codified end state; at the field level it is the design centre of the security roadmap for the two largest protocols by new-node share. For any observer whose method depends on reading control payloads, this category is close to the best case available: the payload remains visible, and the integrity layer strengthens the evidential value of what is observed, since authenticated traffic cannot be trivially spoofed into the observation.

5. The vantage matrix

LTR-2026-04 [1] separated the protocol-independent evaluation core from the channel-contingent observation vantage and asked where, per channel, the evidence for contextual evaluation can be obtained. The landscape assembled above answers that question class by class. Table 1 states the result.

Protocol class	Payload on the wire	Security adoption in practice	Viable observation vantage
Field-level real-time (PROFINET, EtherNet/IP, EtherCAT)	Clear today; signed-but-readable as the security roadmap lands	Protocol-level security largely pre-market; regulation driving capability ahead of activation	Passive mirror; integrity layers strengthen the evidence
Supervisory (OPC UA client-server)	Three modes: clear, signed-readable, encrypted	Deficient configuration measured as the ordinary condition, 2020 and 2025	Passive mirror on None and Sign; legitimate termination or server co-location on SignAndEncrypt; standardised audit events as a secondary source
Energy vertical links (IEC 104, DNP3, IEC 61850 MMS)	Clear; TLS retrofit standardised	Retrofit TLS at 0.4% in the wild; Secure Authentication adoption reported light	Passive mirror for the measurable estate; termination where the TLS retrofit lands
Energy real-time protection (GOOSE, SV)	Signed-but-readable as the codified end state	Authentication extension itself often unused	Passive mirror, permanently, by standard design
Vendor management channels (engineering, HMI, Web APIs)	TLS by default, no clear mode	Default-on in current products; legacy modes persist in the installed base	Legitimate termination point, host co-location, or controller audit logs; authorised active reads for process-state observability
IIoT broker layer (MQTT, Sparkplug B)	TLS positioned as required	Single-digit TLS adoption measured; large unauthenticated broker population	Broker co-location: the terminating component is the native architecture

Table 1. Observation vantage by protocol class. Adoption characterisations summarise Section 3 and carry its evidence labels and its internet-exposure caveat.

Three structural observations follow from the table.

First, the case that motivated the vantage problem in its pure form, an opaque channel with no natural point of legitimate access, occupies one row: vendor management channels. Everywhere else, either the payload remains readable, in three rows including one where readability is the codified end state, or the architecture itself supplies a terminating component at which the traffic is legitimately in clear, as with the broker layer, where the most-encrypted class of OT traffic transits a component that decrypts it by design. Even within the vendor-channel row, secondary sources exist: controllers log control actions through standardised audit mechanisms, and process-state observability through authorised reads was measured directly in the preceding report.

Second, the OPC UA publish-subscribe model of Section 2.2 adds a vantage class that a channel-centric analysis would miss entirely. Because message security rests on symmetric group keys distributed by a key service, an observer admitted to the security group holds the keys to read the traffic without being in its path. Observation access becomes something the architecture can grant, rather than something the observer must seize from a channel. Since the field-level future of OPC UA is built on this model, the point is forward-looking rather than marginal.

Third, encryption does not arrive at a site; it arrives at channels, in a consistent order. Management channels move first and are already there. Vertical supervisory and telecontrol links have the standards but not, measurably, the deployments. The real-time protection plane moves last, or by standard design not at all. An observation architecture designed against "the encrypted site" is designed against something that

does not exist; the real object is a stratified site in which the vantage question has a different answer per plane, and will keep those different answers for a long time.

6. Related observation approaches

Commercial OT network monitoring rests, as an architectural baseline, on passive inspection of mirrored traffic with protocol dissection, extended in current products by three compensating collection methods: targeted active querying of devices in their native protocols, parsing of engineering project and configuration files, and endpoint or ecosystem integrations (vendor-claimed, across the product documentation of the major platforms). Two facts about this category bear on the landscape. The compensating methods recover asset and configuration context rather than per-action visibility, so the passive baseline's blindness under TLS, measured in the preceding report, is not resolved by them. And the commercial acceptance of carefully engineered active querying in production OT environments is itself a data point: strict passivity is no longer the category's admission requirement.

On the academic side, the encrypted-traffic-analysis literature is largely oriented to enterprise traffic and malware detection, working from flow metadata, timing, and handshake features; surveys of the area distinguish three deployment models, interception, cryptographic inspection, and passive inspection without decryption [22] (measured, reported). Two of its results transfer directly to OT. TLS 1.3's mandatory ephemeral key exchange eliminated the passive-decryption deployment model even for an observer holding the server's private key, confirming in the general literature what the preceding report measured on a controller [23] (reported). And the metadata-based detection line shares the structural limitation measured for the volume sensor of the preceding report: it detects anomalous traffic patterns, and an individually valid, well-formed action that is merely inappropriate to its moment does not present as one.

7. Limitations

The evidence base of this briefing has boundaries that its conclusions inherit. The quantitative adoption figures measure internet-exposed populations, and the extension to internal networks is inference, stated as such. The node-share figures for field protocols come from a single recurring vendor analysis of factory automation and exclude the process, energy, and building domains; we treat them as directional. Adoption of PROFINET Security Classes 2 and 3, of CIP Security in the field, and of OPC UA FX cannot yet be measured, because the products are arriving now; statements about them describe specifications and roadmaps, not deployments. The characterisation of commercial monitoring platforms is drawn from public product documentation, and absence of a capability from public materials is weak evidence of its absence from the products. Finally, the vantage matrix states what is observable per class, not what any particular evaluation architecture should do; that selection is design work outside the scope of a landscape study.

8. Conclusion

The empirical question left open by the preceding report has a measured answer. Operational technology is encrypting far more slowly than its standards suggest, the gap between capability and activation is persistent across a decade of measurement, and where security does land on real-time control data, the field's own standards bodies deliberately choose authenticated readability over confidentiality, in one domain codifying that choice as an exclusion of encryption. Encryption reaches OT stratified by functional plane, management channels first and the protection plane last or never, and the pure form of the vantage problem, an opaque channel without a legitimate point of access, is confined to a single protocol class that carries its own secondary evidence sources.

For the research programme Liscere documents, the consequence is direction rather than closure. The observation architecture that the landscape supports is plural by construction: a passive mirror where payloads are readable, which the evidence shows is most of the measurable present and, for some traffic classes, the codified future; a legitimate termination or co-location vantage where transport encryption is real, which the broker layer supplies natively; and granted-key and audit-log sources where the architecture defines them. The preceding report argued that the evaluation core should consume a clean stream of action events independent of its origin. This briefing establishes that no single origin could serve, and that the field, on the evidence, will keep it that way.

References

[1] B. Salmazo. Contextual Evaluation under Encryption. Liscere Technical Report LTR-2026-04, 2026.

[2] HMS Networks. Industrial network market shares 2025. Annual analysis, May 2025.

[3] PROFIBUS and PROFINET International. PROFINET security concept and Security Classes; PROFINET Security Guideline.

[4] ODVA. CIP Security: the cybersecurity network extension for EtherNet/IP. Specification and technology publications, 2021-2025.

[5] EtherCAT Technology Group. EtherCAT and Cyber Security whitepaper; cybersecurity position statements, 2025.

[6] OPC Foundation. General Assembly 2025 highlights; Field Level Communications initiative communications, 2025.

[7] OPC Foundation. OPC Unified Architecture Part 7: Profiles.

[8] OPC Foundation. OPC Unified Architecture Part 14: PubSub.

[9] International Electrotechnical Commission. IEC 62351 series: Power systems management and associated information exchange, data and communications security.

[10] C. Cremers, M. Dehnel-Wild, K. Milner. Secure authentication in the grid: A formal analysis of DNP3 SAv5. Journal of Computer Security 27(2), 2019.

[11] C. Rosborough et al. All About Eve: Comparing DNP3 Secure Authentication With Standard Security Technologies for SCADA Communications. Schweitzer Engineering Laboratories technical paper.

[12] S. M. S. Hussain, T. S. Ustun, A. Kalam. A Review of IEC 62351 Security Mechanisms for IEC 61850 Message Exchanges. IEEE Transactions on Industrial Informatics.

[13] Claroty Team82. Hardcoded cryptographic keys in Siemens SIMATIC S7-1200/1500 and TIA Portal, CVE-2022-38465, 2022.

[14] Siemens. Security concept with TIA Portal V17: secure PG/PC and HMI communication. Application example, Siemens Industry Online Support.

[15] Eclipse Foundation. Sparkplug B Specification, v3.0, 2022.

[16] M. Dahlmanns, J. Lohmöller, J. Pennekamp, J. Bodenhausen, K. Wehrle, M. Henze. Missed Opportunities: Measuring the Untapped TLS Support in the Industrial Internet of Things. Proceedings of the ACM Asia Conference on Computer and Communications Security (AsiaCCS), pp. 252-266, 2022. DOI 10.1145/3488932.3497762.

[17] M. Dahlmanns, J. Lohmöller, I. B. Fink, J. Pennekamp, K. Wehrle, M. Henze. Easing the Conscience with OPC UA: An Internet-Wide Study on Insecure Deployments. Proceedings of the ACM Internet Measurement Conference (IMC), 2020. DOI 10.1145/3419394.3423666.

[18] Bitsight TRACE. OPC UA Server Internet Exposures: 2025 Year in Review. Bitsight Technologies, 2025.

[19] A. Erba, A. Müller, N. O. Tippenhauer. Security Analysis of Vendor Implementations of the OPC UA Protocol for Industrial Control Systems. Proceedings of the 4th Workshop on CPS and IoT Security and Privacy (CPSIoTSec), pp. 1-13, 2022. DOI 10.1145/3560826.3563380.

[20] Modbus Organization. Modbus/TCP Security Protocol Specification, v3.6, 2021.

[21] SunSpec Alliance. Secure SunSpec Modbus Specification.

[22] C. Oh, J. Ha, H. Roh. A Survey on TLS-Encrypted Malware Network Traffic Analysis Applicable to Security Operations Centers. Applied Sciences 12(1):155, 2022.

[23] Challenges and Advances in Analyzing TLS 1.3-Encrypted Traffic: A Comprehensive Survey. Electronics 13(20):4000, 2024.