Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

Read-Only Modbus Data Extraction for IIoT Integration Hardware-Enforced One-Way Telemetry Using Serial Data Diodes and RS-485 Receive- Only Interfaces

Mohammed Shoukatuddin[1], Mohammed Aqheel[2], Mohammed Afzal[3]
[1]Senior Specialist – OT Network & Cybersecurity, Ma'aden Aluminum Company, Saudi Arabia
[2]Senior IT Specialist, Ma'aden Aluminum Company, Saudi Arabia
[3]Specialist I – Systems Administration, Saudi Arabian Mining Company (Ma'aden), Saudi Arabia

Abstract - Many industrial facilities still rely on Modbus RTU at Level 0, a protocol built for trusted, isolated networks that provide no native encryption or authentication. When those sites push telemetry to edge or cloud platforms, the security requirement is typically one-directional: measurements must flow outward, but no control path must exist in return. This paper examines two hardware-enforced methods that satisfy this requirement with minimal operational overhead. The first is a dedicated serial data diode; the second is a physics-enforced RS-485 receive-only interface created by permanently disabling the transceiver driver. Both approaches are explained with reference to DE and /RE control logic, wiring guidance, and reference architectures. A verification checklist and a waiver template for governance purposes are also provided. Either method eliminates the possibility of reverse commands even when the upstream gateway is fully compromised. The final choice between them depends on assurance expectations and site constraints.

Keywords - Modbus RTU; RS-485; one-way telemetry; data diode; receive-only tap; MQTT over TLS; OT cybersecurity; commissioning tests; risk acceptance.

I. INTRODUCTION

Many industrial facilities are expanding their telemetry footprint to support energy optimization, predictive maintenance, and regulatory compliance. In brownfield environments, the lowest instrumentation layer almost always runs Modbus RTU over RS-485. The business need is straightforward—collect field measurements—but the security requirement is more involved: any telemetry path must not create a control capability at Level 0.

A common response is to configure the gateway as read-only. The weakness of that approach is that it depends entirely on software behaving as intended over years of updates, equipment replacements, and vendor changes. It also assumes the gateway will never be turned hostile. In practice, gateways are IT-like assets: they run complex software, expose management interfaces, and are increasingly network-reachable. For critical processes, a better answer is to remove transmit capability at the electrical layer, where it can be inspected, tested, and verified independently of software state.

This paper focuses on two approaches that are both practical and durable. Each enforces a one-way telemetry boundary using hardware, so the protection remains in place regardless of what happens to the gateway software or configuration.

A. Scope and Contribution

The scope covers Modbus RTU over RS-485 at Level 0, feeding an upstream path to an edge or cloud platform via MQTT. Three areas are addressed: a side-by-side comparison of data diodes and physics-enforced receive-only taps; implementation guidance covering DE and /RE control logic and field verification tests; and governance support in the form of a waiver template and risk comparison table.

II. BACKGROUND

Modbus RTU is a request–response protocol designed for trusted, isolated environments. It carries no encryption, no integrity checking beyond a CRC, and no authentication. For decades this was acceptable because field networks were physically separated from everything else. IIoT programmes have changed those assumptions: telemetry is now expected to flow to analytics platforms, sometimes over cellular links or shared infrastructure.

MQTT is a natural fit for the upstream leg because it supports publish–subscribe distribution and is widely supported with TLS transport security. TLS is important, but it does not resolve the fundamental Level 0 concern. If

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

the gateway still has electrical transmit capability on the RS-485 side, it can issue Modbus writes regardless of what is happening on the upstream link. The enforcement point must therefore be the RS-485 interface itself, not the upstream protocol.

A. Gateway Risk in Plain Terms

A protocol gateway occupies the boundary between two very different worlds. On the field side are deterministic buses and legacy instruments; on the network side are full operating systems, remote access, and internet-routable protocols. This creates three concrete risk categories in practice: gradual configuration drift, software defects that alter behavior over time, and deliberate control following a compromise. A hardware-enforced boundary converts all three of those risks into a wiring problem that can be physically inspected and functionally tested.

III. SYSTEM MODEL AND THREAT ASSUMPTIONS

The reference system here consists of Level 0 devices—meters, sensors, and PLC-attached instruments—connected to a shared RS-485 bus. A telemetry gateway reads those devices and publishes measurements to an upstream MQTT broker. Downstream consumers include historians, dashboards, analytics engines, and cloud services.

The threat assumption is deliberately conservative: the gateway is treated as potentially fully compromised. This reflects real-world incident patterns, where edge devices are attractive targets precisely because they bridge trust zones. Under this assumption, software controls are useful but not sufficient. The design objective is strict one-way communication enforced by electrical physics, not by policy.

IV. OPTION 1: DEDICATED SERIAL DATA DIODE

A serial data diode is a purpose-built device that enforces unidirectional data flow at the physical layer. It is installed such that the telemetry path runs outbound only. Once correctly deployed, a compromised gateway may still disrupt telemetry availability, but it cannot issue commands into Level 0.

The main operational advantage is clarity of verification. There is little ambiguity about what the diode does, and commissioning tests focus entirely on confirming direction. This approach suits situations where formal assurance claims, procurement requirements, or regulatory obligations call for a commercial unidirectional solution.

A. Deployment Considerations

Placement is important. In most designs the diode sits at the conduit boundary between the Level 0 field zone and any upstream-connected collector. If an OT DMZ exists, the diode naturally becomes the first enforcement point on the path out of the field zone. The diode does not replace upstream security controls: MQTT should still use TLS, and broker access should require authentication with least-privilege topic permissions.

V. OPTION 2: PHYSICS-ENFORCED RS-485 RECEIVE-ONLY TAP

The second option uses the direction-control logic built into RS-485 transceivers to permanently remove transmit capability. Most half-duplex transceivers expose two control pins: DE (Driver Enable, active-high) and /RE (Receiver Enable, typically active-low). Asserting DE enables the line driver; asserting /RE enables the receiver. By fixing DE low and /RE low in hardware, the interface becomes receive-only at the electrical level.

A. DE and /RE Control Logic

In normal half-duplex operation, a microcontroller GPIO switches the bus direction between transmit and receive by toggling DE and /RE together. A receive-only design removes that GPIO path entirely. DE is tied directly to ground, /RE is tied directly to ground, and DI (the driver data input) is left unconnected or tied to a safe level. With DE permanently low and DI absent, there is no electrical path to drive the A and B lines. The only active output from the transceiver is RO, which feeds the gateway UART receive pin.

B. When This Works (and When It Does Not)

A receive-only tap is best suited to plants where an existing SCADA or PLC master already polls the field bus. The tap simply listens to that traffic and reconstructs register values without generating any bus activity of its own. This is a common arrangement in brownfield sites: a legacy master handles polling, and the monitoring requirement is to mirror those values upstream without interfering.

If the telemetry gateway itself must actively poll devices, a receive-only tap will not work—it cannot generate Modbus requests. In those cases, two alternatives exist: use a diode-based proxy that polls on the trusted side and mirrors measurements outward, or restructure the measurement collection so that all polling stays on the Level 0 side of the boundary.

C. Bus Integrity and Electrical Hygiene

A passive tap must not degrade existing bus performance. The design should respect RS-485 loading rules and

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

should not disturb existing termination resistors. During commissioning, confirm that the communication quality between existing masters and slaves is unchanged with the tap installed. An oscilloscope or protocol analyzer on the bus before and after installation provides a straightforward comparison.

VI. REFERENCE ARCHITECTURES AND WIRING

Figures 1 through 3 show reference architectures and a wiring-level detail for each approach. Figures are sized to fit within a single column to avoid layout problems in publication.

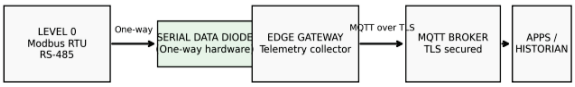

Fig. 1. One-way telemetry using a serial data diode between Level 0 and the collector.

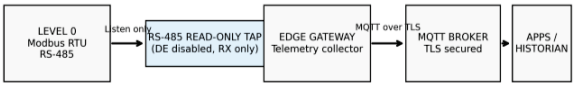

Fig. 2. One-way telemetry using an RS-485 receive-only interface (driver disabled).

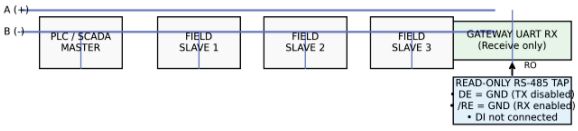

Fig. 3. Wiring concept for a receive-only RS-485 tap (DE grounded; /RE grounded; DI disconnected).

VII. COMMISSIONING AND VERIFICATION Because both options rely on physical enforcement, verification must happen during commissioning, and the results should be documented. For a data diode, confirm that telemetry flows as expected in the outbound direction, then confirm the absence of any reverse signaling path. For a receive-only tap, run a negative test: attempt transmission from the gateway side and verify with a protocol analyzer or oscilloscope that no signal appears on the bus.

Verification should also cover operational hygiene: confirm the tap does not disturb termination or add excessive load to the bus. Upstream integrity is a separate concern. While the gateway cannot reach Level 0 electrically, it can still publish incorrect data if compromised. Broker authentication, topic ACLs, payload sanity checks, and basic anomaly monitoring reduce that residual risk.

VIII. RISK COMPARISON

Table I compares the operational and security trade-offs between the two approaches across several practical criteria.

TABLE I. TABLE I. RISK COMPARISON OF READ-ONLY ENFORCEMENT OPTIONS.

Criteria	Hardware Data Diode	RS-485 Receive-Only Tap
Security assurance	Highest assurance; purpose-built unidirectional device	High assurance; depends on wiring correctness and validation
Reverse command risk	Eliminated by design	Eliminated if DE is disabled and DI is absent
Operational impact	May require inline insertion and outage planning	Often a passive tap with minimal impact
Administration	No ongoing administration	No ongoing administration
Cost	Higher	Lower
Residual risks	False telemetry upstream; gateway availability loss	Physical tampering/wiring error; false telemetry upstream

Table II maps common threats for this telemetry pattern to the controls that address each one.

TABLE II. TABLE II. THREAT-TO-CONTROL MAPPING FOR LEVEL 0 TELEMETRY EXPORT.

Threat	Where it occurs	Recommended control(s)
Modbus write injection	Gateway/collector path	Hardware one-way boundary (data diode or DE-disabled receive-only tap)
Gateway compromise	Gateway OS / services	Least-privilege management access, logging, patch governance; one-way boundary limits impact
False telemetry	Gateway → MQTT broker	TLS + authenticated clients, topic ACLs, payload sanity checks, anomaly monitoring
MQTT credential theft	Broker/client configuration	Mutual TLS where feasible, credential rotation, restricted topics and QoS limits
DoS /	Gateway or broker	Rate limiting,

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

flooding		watchdog/health checks, bounded queues, alerting

IX. NCLUSION

Telemetry projects create security problems when the monitoring path quietly becomes a control path. The cleanest long-term fix is to remove the electrical transmit capability at the boundary, where it can be directly verified and does not depend on any software remaining correctly configured. A dedicated serial data diode and a physics-enforced RS-485 receive-only interface both accomplish this with very little ongoing administration. The decision between them should reflect the site's assurance requirements and physical constraints, and should be supported by documented commissioning tests and well-governed upstream broker controls.

REFERENCES

[1] Modbus Organization, "MODBUS/TCP Security Protocol Specification (MB-TCP-Security-v36_2021-07-30)," 2021.

[2] Y. Ishirara, "A Blind Spot in ICS Security: Protocol Gateway Part 2," Trend Micro Research, 2020.

[3] Y. Ishirara, "A Blind Spot in ICS Security: Protocol Gateway Part 3," Trend Micro Research, 2020.

[4] C. Patel, A. Bashir, A. Alzubi, and R. Jhaveri, "EBAKE-SE: A Novel ECC Based Authenticated Key Exchange between Industrial IoT Devices using Secure Element," Digital Communications and Networks, vol. 9, pp. 358–366, 2022.

[5] Texas Instruments, "Automatic Direction Control RS-485 (TIDA-01090)," 2016.