From Legacy HMI over RDP to Thin Client Manager in Pharmaceutical OT:

Risks • Network Segregation • Access Control • Day-to-Day Support

MSc. Cybersecurity Privacy and Trust

Student: Rafal Rybarski | Email: C00326754@setu.ie | Supervisor: Dr. James Egan

Introduction

Pharmaceutical OT environments require continuous operations, strict governance, and clear separation between network zones. Legacy remote access patterns (HMI over RDP) may persist and can create gaps in segregation, session governance, and supportability. This project evaluates a real migration from a legacy "HMI → preconfigured RDP → host → browser → AMPS" pattern to a brokered Thin Client Manager model in a regulated setting.

Methodology & Evidence

Design: Qualitative, exploratory single-case study

Triangulation of evedence:

Direct artefacts: Technical Design Specification & Site Change Control.

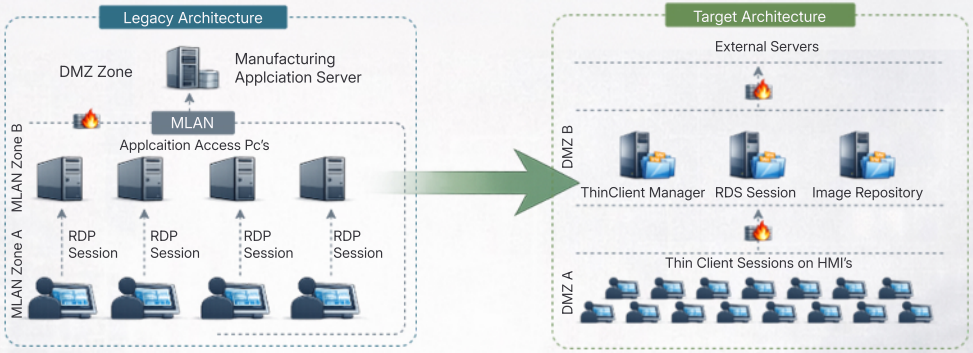
Operational evidence: aggregated ticket metrics.

Indirect evidence: semi-structured interviews across key roles.

Credibility note: interviews are perception-based; direct artefacts and operational metrics provide independent evidence streams.

Before vs After

How does migration from legacy HMI-over-RDP to Thin Client Manager change risk, segregation effectiveness, access/session governance, and support outcomes in regulated pharmaceutical OT?



Early Indications

Preliminary findings suggest that the target model centralises session delivery and strengthens architectural control points. Key evaluation areas include residual gaps in authentication and session governance and operational resilience (failure modes and troubleshooting complexity).

Next Steps

- Conduct semi-structured interviews with key roles.
- Analyse pre/post support ticket trends.
- Compare legacy and target architectures.
- Map findings to OT security principles.
- Develop evidence-based conclusions.

References

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H. and Stoddart, K. (2016) 'A review of cyber security risk assessment methods for SCADA systems'. Computers & Security, 56, pp. 1-27. doi:10.1016/j.cose.2015.09.009.

CISA (2023) Configuring and Managing Remote Access for Industrial Control Systems (ICS): Recommended Practice. Washington, DC: Cybersecurity and Infrastructure Security Agency. Available at: https://www.cisa.gov/sites/default/files/2023-01/RP_Managing_Remote_Access_S508NC.pdf (Accessed: 22 October 2025).

Knowles, W., Prince, D., Hutchison, D., Disso, J. and Jones, K. (2015) 'A survey of cyber security management in industrial control systems'. International Journal of Critical Infrastructure Protection, 9, pp. 52-80. doi:10.1016/j.ijcip.2015.02.002.

National Institute of Standards and Technology (NIST) (2023) Guide to Operational Technology (OT) Security. NIST Special Publication 800-82 Rev.3. Gaithersburg, MD: NIST. doi:10.6028/NIST.SP.800-82r3.

Research Questions

Migration impact on OT security risk profile.

Segregation improvement and residual gaps.

Access control & session governance differences and mitigations.

Day-to-day support impact (ticket trends and recurring categories)

Operational & Security Impact

Shift from direct RDP access to brokered sessions introduces controlled and auditable access paths.

Clear separation between MLAN and DMZ improves enforcement of security boundaries.

Reduction of workstation dependency decreases operational risk and simplifies troubleshooting.

Centralised session management supports more consistent and scalable OT support practices.