

PROJECT ANVIL

Worked remediation costing · Finding F1 · From finding to deal term

This is a single finding taken end to end. It shows how one observation becomes a cost, a timeline and a position at the negotiating table. The same method is applied to each finding and rolled up into the total remediation figure carried in the investment committee summary.

1. The finding

There is no segmentation between the corporate IT network and the plant control networks at any of the six manufacturing sites. Engineering workstations, historians and human-machine interfaces sit on the same flat domain as office file servers and the finance estate. Vendor remote access terminates inside the same network. A single set of domain credentials reaches from an office laptop to a programmable logic controller.

Nothing here is exotic. This is the most common finding in industrial diligence and it is the one most often recorded as a technical observation and then dropped from the commercial narrative.

2. Why it matters commercially

- A commodity ransomware event on the corporate estate, the kind this business already experienced in 2024, propagates to production. The company is not being targeted. It does not need to be.
- Recovery of OT systems from vendor media, which is what happened in 2024, took eleven days at one site. Across two sites in peak season the modelled loss is €14m to €31m in lost contribution, expedited freight and contractual penalties.
- The four largest customers now require evidence of network segmentation at supplier audit. Two contracts, representing €38m of revenue, carry a right to audit that has not yet been exercised.
- At exit, a sophisticated buyer will run the same diligence. An unsegmented estate is a visible discount. Fixing it in year one converts a discount at exit into a credential.

3. Cost to remediate

Costed to a defensible position, not to a best-practice ideal. The scope is zone separation with controlled conduits, monitored vendor access and proven recovery. It is not a full Purdue model rebuild, which would cost roughly three times this and would not change the risk position materially inside a hold period.

Workstream	One-off	Annual run-rate	Basis of estimate
OT asset discovery and network mapping, six sites	€160k	–	Passive discovery tooling plus 4 weeks of specialist effort per cluster
Segmentation design and reference architecture	€85k	–	One design, applied six times. Not six designs
Industrial firewalls, switching and data diodes	€560k	€78k	Six sites, 3 zones per site. Vendor list price less typical discount
Implementation and commissioning	€290k	–	Two plants per wave, executed in scheduled maintenance windows
Managed remote access platform for OEM vendors	€85k	€42k	Replaces 14 uncontrolled vendor connections
Monitoring extension into the OT estate	€55k	€165k	Sensor deployment plus 24/7 coverage through a managed provider
Two OT security engineers	–	€190k	Loaded cost, Poland and Germany. Permanent capability, not project
Programme management and assurance, 14 months	€110k	–	0.5 FTE programme lead plus independent design review
Total, finding F1	€1.35m	€475k	Range €1.15m to €1.60m including contingency

Estimates are built from comparable programmes delivered in multi-site industrial environments. They assume the target's own engineering resource is available for plant coordination. They exclude any equipment replacement driven by obsolescence rather than security, which is a separate capital question for the operational team.

4. Time to defensible

Fourteen months for this finding. The constraint is not money and it is not skills. It is production downtime. Segmentation cannot be cut over while a line is running, and this business has four scheduled maintenance windows per year across six sites. That single fact sets the shape of the plan.

Months	Activity	Binding constraint	Risk reduced
0 – 2	Discovery, asset inventory, design	Specialist availability	None yet
2 – 4	Procurement and staging	Industrial switching lead times, 10 to 14 weeks	None yet
3 – 9	Plant implementation, two per wave	Scheduled maintenance shutdowns only	60%
9 – 11	Vendor remote access and OT monitoring	OEM contract renegotiation	85%
11 – 14	Validation, tabletop exercise, evidence pack	Nothing external	100%

Sixty percent of the risk is removed by month nine. That matters more than the completion date. A sponsor with a hold period should know when the exposure stops being existential, not just when the programme closes.

5. Effect on price

Two costs, argued two different ways. Conflating them is the most common error in cyber diligence and it usually costs the buyer money.

Permanent run-rate cost	€475k per year	Monitoring, licensing, maintenance and two engineers. This does not go away.
Applied to entry multiple	9.0x	The recurring cost reduces normalised EBITDA at the multiple being paid.
Enterprise value effect	€4.28m	The valuation argument. This is the number the seller will contest.
One-off capital cost	€1.35m	Argued separately as a cash item, not an EBITDA adjustment.
Total opening position, F1	€5.63m	Against a €234m enterprise value. Roughly 2.4% of EV from one finding.

How this is argued

- Lead with the run-rate, not the capital. Sellers expect a capex conversation and are prepared for it. The permanent EBITDA effect is the larger number and is harder to dismiss because it is arithmetic on their own multiple.
- Separate the two engineers from the hardware. Headcount is the line a seller will attack as buyer preference rather than necessity. It is defensible here because the estate cannot be operated safely without it, and because the target's own insurance renewal already assumes the capability exists.
- Do not ask for the full number and do not open with a range. Open at €5.63m for this finding, with the build shown. A costing that can be walked line by line survives challenge. A round number does not.
- Expect to land between 55 and 70 percent of the ask, with the balance addressed through a specific indemnity for the 2024 incident rather than through price.

What would change this number

- Two of the six sites were not visited. If their OT estate matches the visited sites, the estimate holds. If either runs a materially different control platform, the hardware line moves by up to €200k.
- Industrial switching lead times have moved between eight and twenty weeks over the past two years. A longer lead time does not change cost, but it extends time to defensible by up to a quarter.
- If the sponsor intends to bolt on further sites during the hold, designing for that now adds roughly €90k and avoids a repeat programme later.
- If the seller has already committed capital to this work, which management indicated but did not evidence, the one-off cost reduces and the argument shifts to timing and completion risk rather than quantum.

This document is an illustration of method. Figures relate to a fictionalised target and are not derived from any client engagement. Ranges are indicative for negotiation and are not quotations or a warranty of outcome.