



INDUSTRY BRIEF

Segmenting IT from OT Without Stopping the Line

A staged approach to industrial network segmentation for plants that cannot take downtime, mapped to the IEC 62443 zone-and-conduit model.

PUBLISHED

April 15, 2026

READING TIME

11 minutes

AUTHOR

SCIAT AFRICA Research

ABSTRACT

Manufacturing and utility environments carry the hardest version of the segmentation problem: the networks that most need isolating are the ones that cannot be taken offline to do it. This brief sets out a staged approach that produces real containment without a plant shutdown, using the zone-and-conduit model from IEC 62443 as the organising frame.

Topics: OT Security · Network Architecture · Manufacturing

WHAT TO TAKE AWAY

- Start with visibility: passive monitoring tells you what actually talks to what, which is almost never what the diagram says.
- Remote vendor access is the most common uncontrolled conduit into an OT network.
- A single engineering workstation with dual connectivity undoes a great deal of expensive segmentation.
- Enforcement can be staged – monitor, then alert, then block – so that nothing stops the line unexpectedly.
- IEC 62443's zones and conduits give you a vocabulary that both plant engineering and IT security can agree on.

CONTENTS

- 01 Why the usual advice does not land
- 02 Stage one: see the traffic before you change anything
- 03 Stage two: zones and conduits on paper
- 04 Stage three: enforce in increments
- 05 The two exceptions that undo everything

01 Why the usual advice does not land

Enterprise segmentation guidance assumes you can change a firewall rule, observe what breaks, and roll back. On a production line that assumption does not hold: the cost of an unplanned stop is measured in lost output and sometimes in safety, and the equipment may be running software that cannot be patched, restarted casually, or in some cases even scanned.

The result is a widespread pattern of plants that are nominally segmented – there is a firewall between the business network and the plant network – while in practice carrying a long list of exceptions, a flat plant network behind that firewall, and vendor remote access that bypasses it entirely.

02 Stage one: see the traffic before you change anything

Passive network monitoring on span or tap ports changes no configuration and risks nothing on the control network, and it reliably contradicts the documentation. In almost every assessment we find flows nobody expected: a historian reaching the internet for updates, a vendor laptop with a persistent tunnel, a controller talking directly to a business-network server, an engineering workstation bridged to both networks at once.

Four to six weeks of observation across a full production cycle, including a maintenance window, gives you the real communication matrix. Everything afterwards is cheaper and safer because of it.

03 Stage two: zones and conduits on paper

IEC 62443 models an industrial system as zones – groupings of assets with a shared security requirement – connected by conduits, which are the controlled paths between them. The model is useful here because it is a shared language: plant engineering thinks in process areas and criticality, IT security thinks in trust boundaries, and zones and conduits map cleanly onto both.

In practice the first cut is usually: enterprise, a demilitarised zone for the systems that legitimately need to exchange data in both directions, supervisory control, basic control, and safety instrumented systems as their own zone with the tightest constraints. Every flow you observed in stage one is then either assigned to a conduit or marked for removal.

- Define zones by shared security requirement and consequence of failure, not by physical location.
- Make every permitted flow an explicit conduit with a named owner and a business reason.
- Put all enterprise-to-plant data exchange through a demilitarised zone; no direct flows.
- Treat safety systems as a separate zone with no routine conduit to anything else.

04 Stage three: enforce in increments

Deploy the enforcement points in monitor mode first, so they report what they would have blocked without blocking it. Review that report with plant engineering, resolve the surprises, then move to alert, then to block one conduit at a time, each during a planned window with a rollback that has been tested.

This is slower than a single cut-over and it is the reason the work actually completes. Segmentation projects on production networks fail far more often from one unplanned stoppage destroying organisational confidence than from technical difficulty.

05 The two exceptions that undo everything

Vendor remote access is the most common uncontrolled conduit we find. Equipment suppliers legitimately need to reach their machines, and the arrangements are frequently older than the current security programme: a cellular modem installed by the vendor, a persistent tunnel, shared credentials, no logging. Bring every one of these into a single brokered path – authenticated per engineer, time-bound, session-recorded, approved per access.

The second is the dual-homed engineering workstation. A laptop connected to both the plant network and the business network is a routed path regardless of what the firewall says, and the same applies to removable media carried between zones. These need to be addressed by policy and by host configuration, because no amount of network architecture compensates for them.

About this publication

This document is published by SCIAT AFRICA, a cybersecurity and digital forensics agency based in Nairobi, Kenya. It is free to read, print and circulate inside your organisation. The web edition, which carries the same content, is at <https://sciatafrica.com/research/ot-network-segmentation-brief>.

It is general guidance, not legal advice and not a substitute for an assessment of your own environment. Where it refers to a law, regulation or standard, read the instrument itself before relying on it – and talk to us if you want help applying it to your estate.

SCIAT AFRICA

info@sciatafrica.com · +254 794 946633 · <https://sciatafrica.com>