VALIANT COMMUNICATIONS

VCL Network Isolation

(Kill Switch) Equipment

Hardware-Based Network Isolation for Defence,
Power Utilities & Critical Infrastructure

Last-Line-of-Defence · Fail-Safe · Hardware-Level · Deterministic Isolation

The Cyber Threat Landscape

Why firewall-only defences are insufficient for critical infrastructure

Ransomware & Malware

Ransomware attacks encrypt critical OT/IT data and hold operations hostage. Malware can traverse firewall boundaries via zero-day exploits, lateral movement, or compromised credentials — shutting down power grids, defence networks and industrial systems.

DDoS & Network Floods

Distributed Denial-of-Service attacks saturate WAN links, disabling communications between control centres and field assets. Legacy firewalls cannot maintain stateful inspection under high-volume floods while also enforcing policy.

Advanced Persistent Threats

APTs quietly infiltrate OT networks through the IT-OT boundary, exfiltrating data and pre-positioning for sabotage. The 2015 Ukraine power attack and Operation Buckshot Yankee both bypassed firewall-only perimeters.

KEY INSIGHT: A firewall can be compromised. A hardware kill switch cannot — it operates at the physical layer, creating an assured, deterministic disconnect that no software exploit can bypass.

VCL Network Isolation (Kill Switch) Equipment

The last-line-of-defence for OT/IT network separation

Hardware-Level Isolation

Physical-layer LAN/WAN disconnect — no software exploitable path. Operates independently of host OS, firewall state or control plane.

Fail-Safe Architecture

Maintains configured state (isolated or connected) even during power failure or control card failure. Never itself becomes a point of failure.

Automatic + Manual Modes

Triggered automatically via SNMP traps, dry-contact relays, RS-232/RS-485 scripts, or manually via front-panel override switch.

Full Audit Trail

All events time-stamped, logged and stored in non-volatile memory. SNMP traps sent to centralised NMS for full accountability.

Works with Any Firewall

Vendor-agnostic. Integrates with Cisco, Fortinet, Palo Alto, Check Point or any firewall that can generate SNMP traps or dry-contact outputs.

VCL-2702 · VCL-5052 · VCL-5054

1G Electrical · 1G/10G Optical · Quad-Port 1G/10G

VCL-2702	VCL-5052	VCL-5054
1U, 1G Elec. 1-Port	1U, 1G/10G Opt. 1-Port	2U, Quad-Port 1G/10G

Key Features & Isolation Trigger Methods

Multiple independent activation paths ensure reliable response under any attack scenario

ISOLATION TRIGGER METHODS

SNMP Trap (v2)

Cisco ASA 5585 or any SNMP-capable firewall/IDS sends trap OID → automatic isolation. Tested & validated with Navy PoC.

Dry-Contact Triggers (8-pin)

External relay contacts (open/close) from fire alarm panels, physical intrusion detectors or SCADA systems trigger instant isolation.

RS-232 / RS-485 Out-of-Band

Scripted commands via serial out-of-band access provide isolation control fully independent of the main network — even if WAN/LAN is compromised.

Manual Override Switch

Front-panel Fail-Safe manual switch provides deterministic human-operator kill — critical in scenarios where automated triggers are unavailable.

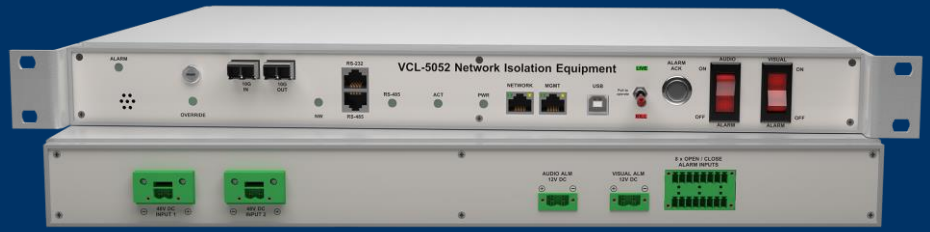
ACTIONS ON ISOLATION TRIGGER

- Physically disconnect LAN from WAN (hardware relay opens)
- Isolate specific SAN/NAS data storage from local network
- Activate Audio Alarm (configurable decibel alert)
- Activate Visual Alarm (12V DC external indicator)
- Send network security alerts to administrators
- Log event with precise timestamp to non-volatile memory
- Trigger external intrusion detection alarm indicators

Fail-Safe: Maintains isolation state even on power loss or control card failure — physically impossible to bypass remotely.

Hardware Portfolio

VCL-2702 · VCL-5052 · VCL-5054 | 1U & 2U 19-inch Rack Mount



	VCL-2702 Single-Port 1G	VCL-5052 Single-Port 1G/10G	VCL-5054 Quad-Port 1G/10G
Form Factor	1U, 19-inch Rack	1U, 19-inch Rack	2U, 19-inch Rack
Interface	1G Electrical (RJ45)	1G/10G Optical (SFP+)	4×1G Opt or 4×10G Opt
Validated	Navy, Global	ONGC, Grid India, Global	ONGC, Grid India, Global
Power	<18W, 48V DC dual	<18W, 48V DC dual	<22W, 48V DC dual
Dry-Contact Inputs	8-pin alarm inputs	8-pin alarm inputs	8-pin alarm inputs
Serial Interfaces	RS-232 + RS-485	RS-232 + RS-485	RS-232 + RS-485
Weight	<2.5 kg	<2.5 kg	<3.7 kg

Navy PoC — Satisfactory Testing & Validation

VCL Network Isolation (Kill Switch) Equipment — Proof of Concept

PROOF OF CONCEPT — ALL TESTS PASSED

Equipment: 8-port hardware (VCL-5054) — 4 Network Ports, 4 Protected Ports — supporting 1G/10G
Configuration: VCL Network Isolation (Kill Switch) Equipment installed inline between WAN and LAN. SNMP trap monitoring from Cisco ASA 5585 Firewall. On receipt of predefined trap OIDs → automatic LAN/WAN isolation.

1	**Manual Fail-Safe Switch** Instant physical isolation triggered — confirmed by visual/audio alarm	✓ PASS
2	**SNMP Trap (v2)** Cisco ASA 5585 trap OID received → automatic LAN/WAN disconnect	✓ PASS
3	**RS-232 Serial Out-of-Band** Scripted commands via RS-232 triggered isolation successfully	✓ PASS
4	**RS-485 Serial Out-of-Band** Scripted commands via RS-485 triggered isolation successfully	✓ PASS
5	**8-Pin Dry-Contact Triggers** All 8 contact inputs validated — each triggered correct isolation	✓ PASS
6	**Audio & Visual Alarms** 12V DC audio and visual alarms activated on isolation event	✓ PASS

CONCLUSION: The VCL Network Isolation (Kill) Equipment successfully met all PoC objectives — effective hardware-level isolation, controlled data flow and stable performance under all tested trigger methods.

Navy PoC — Satisfactory Testing & Validation

VCL Network Isolation (Kill Switch) Equipment — Proof of Concept

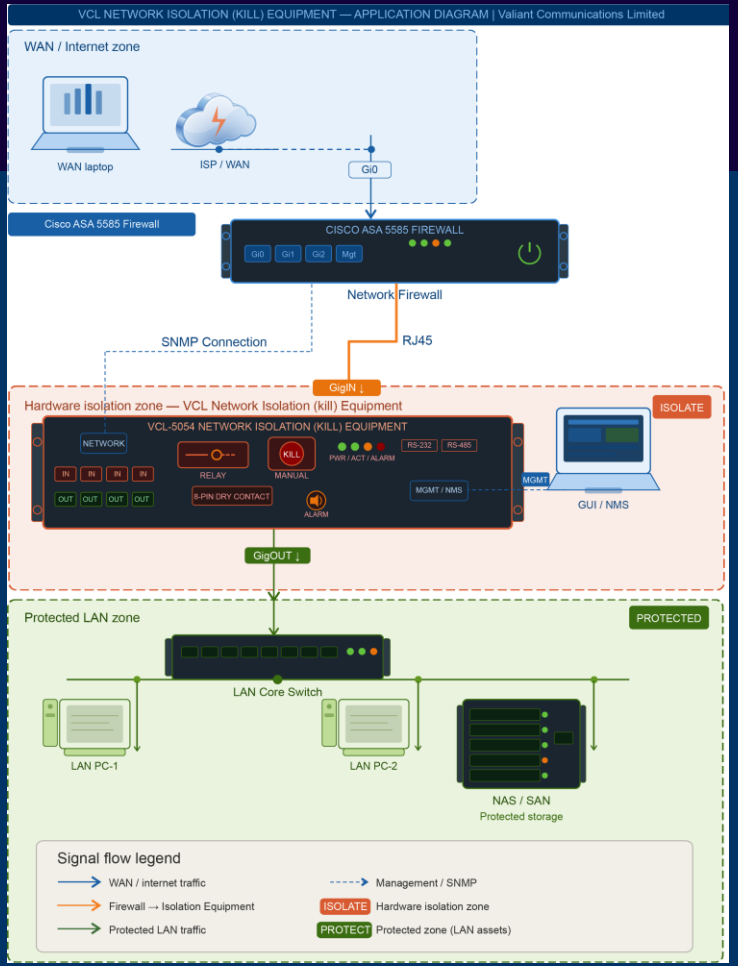
PoC NETWORK TOPOLOGY

Defence & Military

- Disconnect combat networks from admin on threat detection
- Enforce air-gap for classified systems (OT isolation)
- DRDO/MoD classified/unclassified network boundary
- Shipborne / airborne mission-critical network isolation

Banking, Finance & Data Centres

- Isolate payment processing from trading networks
- Air-gap backup NAS/SAN from main LAN on ransomware
- Isolate HSM (Hardware Security Module) segments
- SWIFT network isolation from corporate IT



CONCLUSION: The VCL Network Isolation (Kill) Equipment successfully met all PoC objectives — effective hardware-level isolation, controlled data flow and stable performance under all tested trigger methods.

Sector Applications

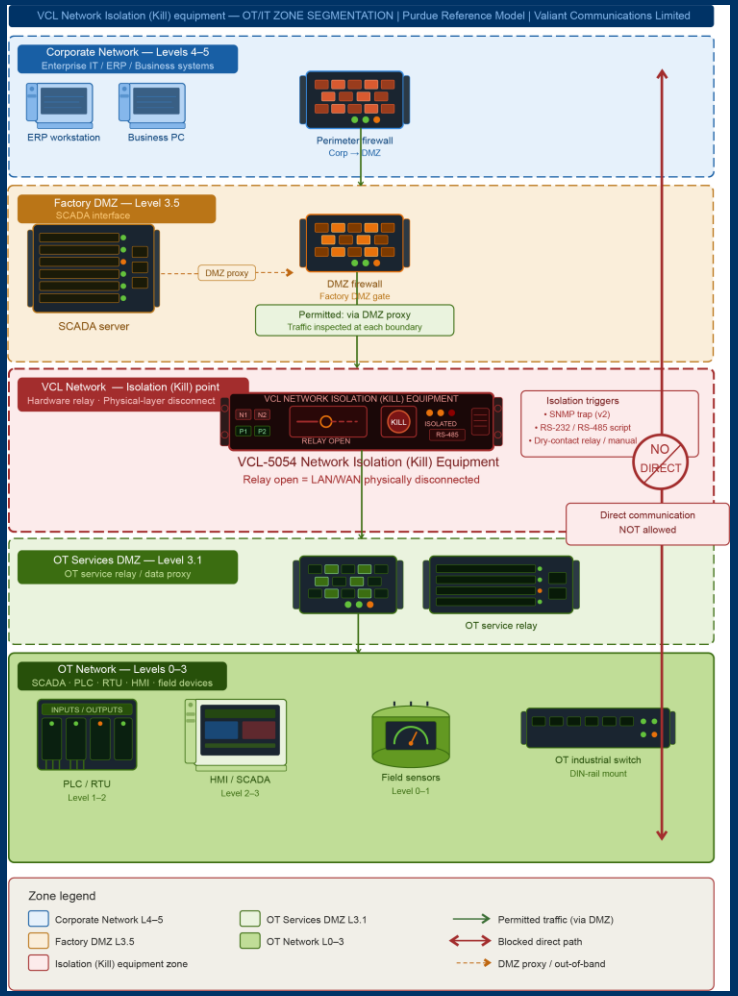
Defence · Power Utilities · Critical National Infrastructure · Banking · Telecom

Power Utilities (220kV–HVDC)

- IT/OT boundary isolation at EHV substations
- Isolate SCADA historian from corporate network
- NERC CIP-005 electronic security perimeter enforcement
- Protect protection relay systems from IT-side attacks

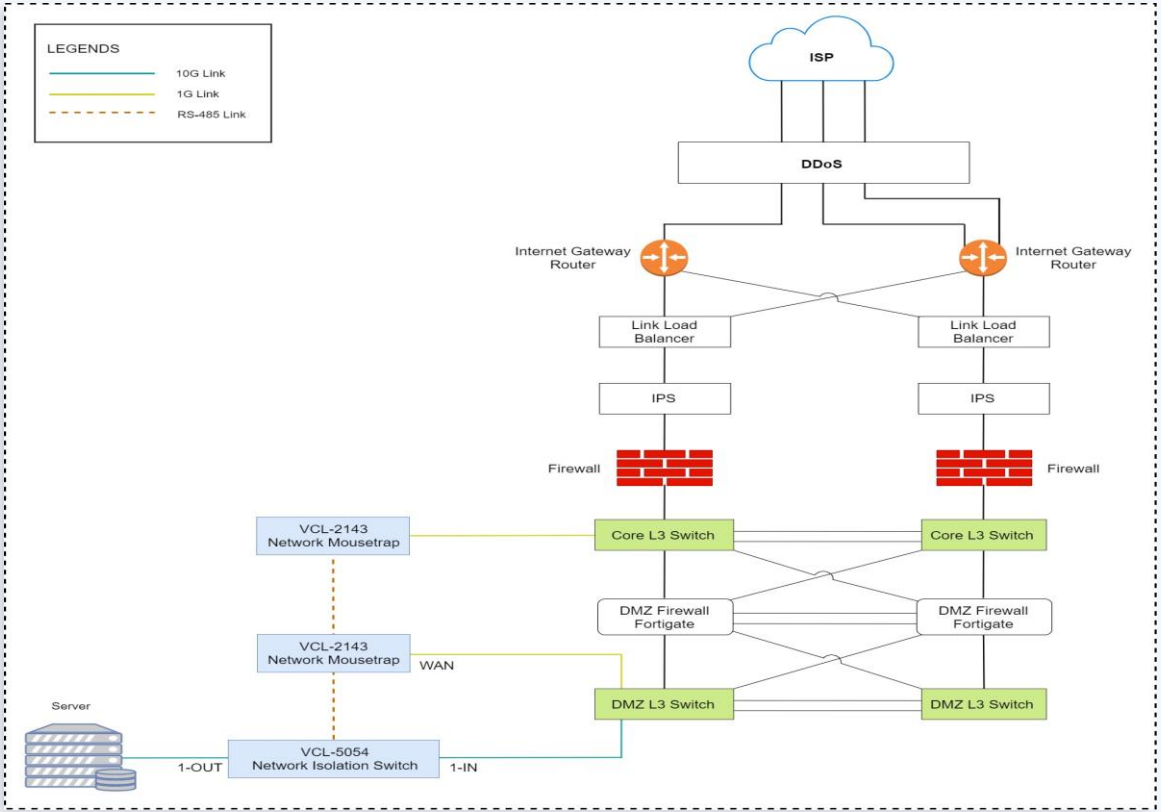
Oil & Gas / Railways / Telecom

- Pipeline SCADA isolation from corporate WAN
- Railway ATP/ATC network segmentation from IT
- Telecom 5G core isolation from internet-facing infra
- Airport ATC network isolation from passenger WiFi



Network Application Diagram

VCL Network Isolation (Kill Switch) Equipment deployed inline between WAN and protected LAN zones



ISP / WAN Perimeter

Dual Internet Gateway Routers with DDoS scrubbing. Network Isolation Equipment sits downstream of firewalls — ensuring hardware disconnect preserves internal mission networks even when perimeter is overwhelmed.

VCL-2143 Mousetrap Integration

Network-MouseTrap honeypot devices detect lateral movement and intrusion. On alert, they send SNMP trap OID to the Network Isolation (Kill) Equipment — triggering automatic isolation without human intervention.

VCL-5054 Network Isolation (Kill) Equipment (Inline)

Installed between DMZ L3 switches and protected LAN/server segment. Provides hardware-layer disconnect — no software path survives. Server and SAN storage remain protected even under active attack.

IP addresses masked in production deployment. Works with any vendor firewall.

Three Repeatable Deployment Patterns

Aligned with NIST SP 800-82, NSA network segmentation guidance and ICS-CERT best practices

1 Edge Isolation

Disconnect external links,
preserve internal mission network

Network Isolation (Kill Switch) Equipment installed between WAN/internet uplink and internal network. On cyber event: external link severed instantly while internal LAN, OT systems and comms continue operating. Directly implements NIST SP 800-82 perimeter/DMZ layering and NSA's principle that a compromised external link must not propagate inward.

Use cases: ISP-facing routers, border firewalls, satellite uplinks, SCADA historian internet feeds

2 Zone Segmentation

Disconnect between internal zones
(Combat↔Admin, OT↔IT, DMZ↔Core)

Network Isolation (Kill Switch) Equipment installed between internal network zones (IT/OT boundary, combat network/admin network, classified/unclassified). NSA explicitly states physical separation is stronger than logical because the intermediate device must itself be compromised to bypass restrictions. Enables zone containment without relying on VLAN or ACL integrity.

Use cases: Power substation IT/OT boundary, MoD classified/unclassified, production/corporate

3 Air-Gap Enforcement

Default disconnected; connect only for
authorised, time-bounded operations

Network is physically disconnected by default. Network Isolation (Kill Switch) Equipment closes the connection only during approved maintenance windows (patching, data transfer, backup). Critical given Buckshot Yankee (2008) — infected USB media bridged an 'air-gapped' DoD network — and Ukrainian ICS compromises where attackers pre-positioned via IT/OT bridge connections.

Use cases: Classified military networks, nuclear facility control, critical OT historian backup

Operational Lessons: Why Assured Disconnect Matters

High-impact cyber incidents that demonstrate the critical need for hardware-level network isolation

2015

Ukraine Power Grid Attack

Threat Actor: SANDWORM / APT28

Attackers used spear-phishing to enter IT networks, traversed the IT/OT boundary, and issued unauthorised commands to SCADA systems via legitimate protocols. 230,000 customers lost power for up to 6 hours. Critically: the attackers also launched a telephony DDoS to prevent customers reporting outages and rendered SCADA workstations inoperable with Kill Disk malware.

Network Isolation (Kill Switch) Equipment Lesson:
A hardware network isolation (kill) equipment between the IT/OT boundary would have severed the attacker's control path to substations before commands could reach field devices.

2008

Operation Buckshot Yankee

Threat Actor: AGENT.BTZ / APT (attributed Russia)

An infected USB memory stick introduced malware ('agent.btz') to a DoD laptop on a classified network. The malware bridged the 'air-gapped' SIPRNet — the DoD's secret network — creating unauthorised exfiltration channels. This led to the establishment of US Cyber Command and the creation of NIST SP 800-171.

Network Isolation (Kill Switch) Equipment Lesson:
Time-bounded, hardware-enforced air-gap closure (Pattern 3) with physical-layer disconnect would have prevented the bridging of the classified network via removable media.

2021+

Power Grid & Critical Infra Attacks (India & Global)

Threat Actor: Multiple APTs

RedEcho (linked to China) targeted 10 Indian power sector organisations including NTPC, SEB load dispatch centres and a nuclear power plant. Volt Typhoon (US) and Fancy Bear (Europe) have pre-positioned in ICS networks. Colonial Pipeline (US) ransomware caused fuel shortage across US East Coast after IT/OT pivot.

Network Isolation (Kill Switch) Equipment Lesson:
Hardware network isolation (Kill Switch) equipment provide the deterministic, physical-layer barrier that prevents APT lateral movement from IT to OT — a boundary that firewall policy alone cannot reliably enforce.

Hardware Isolation vs Firewall-Only Architecture

Comparative analysis for Transmission Substations (220kV / 400kV / 765kV / HVDC)

Criterion	Firewall-Only Architecture	VCL Hardware Network Isolation (Kill) Equipment + Firewall
Exploit Resistance	Vulnerable to OS/software zero-day exploits, misconfiguration, and FW rule bypass	Physical relay — no software exploitable path. Cannot be remotely compromised
Isolation Certainty	Logical isolation (VLAN/ACL/policy) — can be overridden by privileged attacker	Deterministic physical disconnect — 100% guaranteed at hardware layer
Fail Behaviour	FW failure may default OPEN (pass traffic) — dangerous in attack scenario	Fail-safe: maintains last configured state (isolated) on power/card failure
IEC 62351 / NERC CIP	Partial compliance — logical controls; regulators increasingly require physical controls	Supports full NERC CIP-005/007 physical separation and IEC 62351 zoning
Response Speed	Policy evaluation + stateful inspection latency (ms to seconds)	Hardware relay triggers in <50ms — sub-cycle for protection relay systems
Audit Trail	FW logs (may be altered if attacker has admin access)	Non-volatile hardware log — tamper-resistant, SNMP trap to NMS
OT Protocol Awareness	Requires DPI for Modbus/DNP3/IEC 61850 (complex, license costs)	Protocol-agnostic — isolates any Ethernet segment regardless of protocol
Single Point of Failure	Yes — FW compromise = network compromise	No — operates independently; never itself becomes a failure point

Defence-in-Depth: Regulatory & Standards Alignment

NIST · NSA · CISA · ICS-CERT · DAP 2020 · MoD/DRDO procurement norms

NIST — SP 800-82 Rev.3 — **OT Security**

Recommends network segmentation with hardware barriers between zones. NIST SP 800-171 (DoD supply chain) mandates physical access controls and network separation for CUI systems.

NSA — Network Segregation Guidance — **Physical Separation**

NSA explicitly states: physical separation provides STRONGER protection than logical controls because the intermediate device must itself be compromised to bypass restrictions — directly aligning with network isolation (kill) equipment deployment.

CISA — ICS-CERT Advisories & CIPAC Guidance — **ICS/SCADA**

CISA recommends that all ICS/SCADA systems be isolated from corporate networks using hardware controls. Kill switches implement the 'Controlled Interface' pattern in CISA's cross-domain solution guidance.

MoD / DAP 2020 — Defence Acquisition Procedure 2020 — **India Defence Procurement**

DAP 2020 Chapter II specifies indigenous content requirements and technology security for defence networks. VCL Network Isolation (Kill) equipment (Made in India) satisfies hardware-based network security requirements for classified defence network segmentation under MoD/DRDO norms.

NERC CIP 005/007 — Critical Infrastructure Protection Standard — **Power Utilities**

NERC CIP-005 (Electronic Security Perimeters) and CIP-007 (Systems Security Management) require physical controls at substation IT/OT boundaries — not merely logical/firewall controls. Kill switches directly implement CIP-005 'Electronic Access Control'.

IEC 62351 IEC 61850 — Power System Cyber Security — **Substations**

IEC 62351-4/5/7 specifies authentication and access control for IEC 61850 (substation automation) communications. Hardware isolation provides physical containment that complements IEC 62351 cryptographic controls.

Securing Critical Networks

VCL Network Isolation (Kill Switch) Equipment

- Hardware-layer physical disconnect — no software exploit can bypass
- Fail-safe — maintains isolation state even on power or card failure
- Validated by Navy PoC across all 6 trigger methods
- Aligned with NIST SP 800-82, NSA, CISA, NERC CIP, DAP 2020, IEC 62351
- Three deployment patterns: Edge isolation · Zone segmentation · Air-gap enforcement
- Vendor-agnostic. Integrates with Cisco, Fortinet, Palo Alto, or any firewall.

U.S.A.

Valcomm Technologies Inc.
4000 Ponce de Leon Blvd.,
Suite 470, Coral Gables, FL 33146,
U.S.A.
E-mail: us@valiantcom.com

U.K.

Valiant Communications (UK) Ltd.
Central House Rear Office,
124 High Street, Hampton Hill,
Middlesex TW12 1NS, United Kingdom
E-mail: gb@valiantcom.com

INDIA

Valiant Communications Limited
71/1, Shivaji Marg,
New Delhi - 110015,
India
E-mail: mail@valiantcom.com

www.valiantcom.com