

BÁO CÁO CHIẾN LƯỢC BẢO MẬT HẠ TẦNG TRỌNG YẾU



ẢO ẢNH CỦA DATA DIODE & XU HƯỚNG CÔNG NGHỆ TƯƠNG LAI

Giải pháp Cách ly Điện tử (Electronic Isolation)
trong bảo vệ Hạ tầng Thông tin Trọng yếu Quốc gia.

\$8.4

NGHÌN TỶ USD

Thiệt hại do tội phạm
mạng toàn cầu (2023).



Quốc phòng



Tài chính - Ngân hàng



Năng lượng



Chính phủ

Các hạ tầng này là xương sống của quốc gia. Một lỗ hổng nhỏ có thể dẫn đến thảm họa an ninh và kinh tế.

KẾT NỐI ĐỂ PHÁT TRIỂN



CÁCH LY ĐỂ SINH TỒN



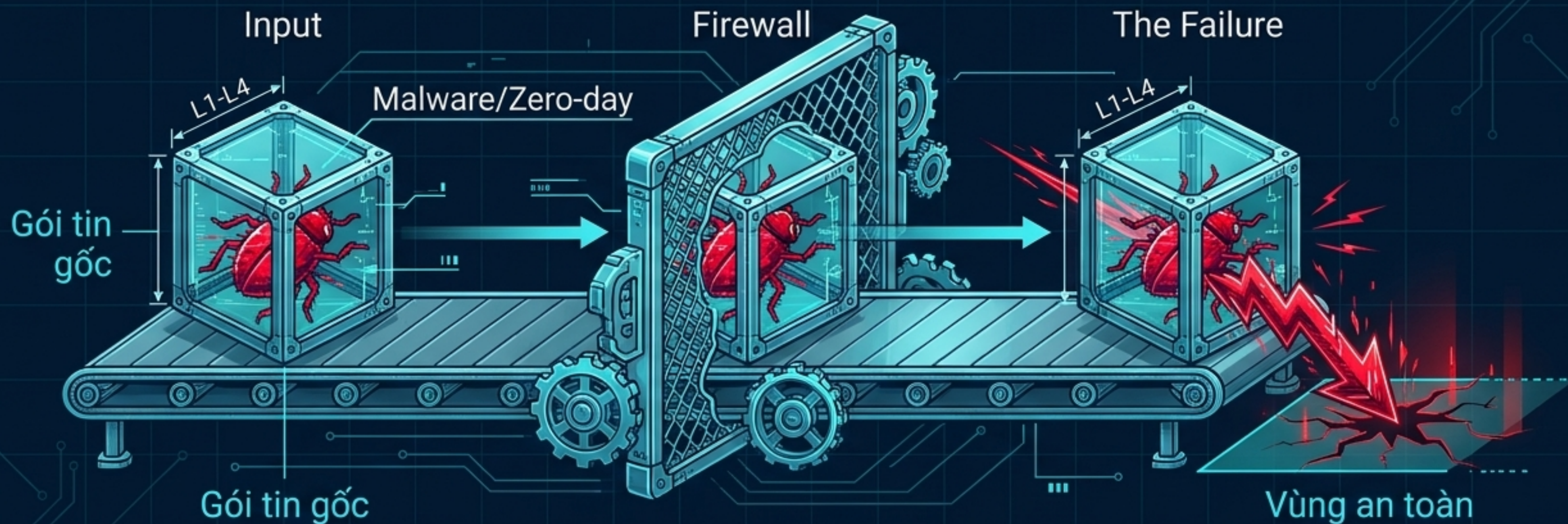
**NGHỊCH LÝ HÓC BÚA:
LÀM THẾ NÀO ĐỂ VỪA CÁCH
LY HỆ THỐNG TUYỆT ĐỐI,
VỪA ĐẢM BẢO DÒNG DỮ LIỆU
HAI CHIỀU THỜI GIAN THỰC?**

Yêu cầu chuyển đổi số: Dữ liệu xuyên suốt, đồng bộ thời gian thực, đa giao thức.

Yêu cầu an ninh: Ngăn chặn APT, ransomware, bảo vệ vùng lõi tuyệt đối.

SỰ BẾ TẮC CỦA TƯỜNG LỬA: CHỈ LỘC, KHÔNG CÁCH LY

Tường lửa giữ nguyên cấu trúc gói tin gốc (L1-L4) và duy trì kết nối mạng trực tiếp.



Kẻ tấn công dễ dàng khai thác lỗi TCP/IP stack (Ripple20, IPnet) hoặc Zero-day để xuyên thủng hệ thống mà không cần phá vỡ quy tắc lọc.

RÀO CẢN CỦA AIR GAP: AN TOÀN NHƯNG CÔ ĐỘC

Tê liệt chuyển đổi số.
Tạo ra các "hòn đảo dữ liệu", không thể đồng bộ thời gian thực.

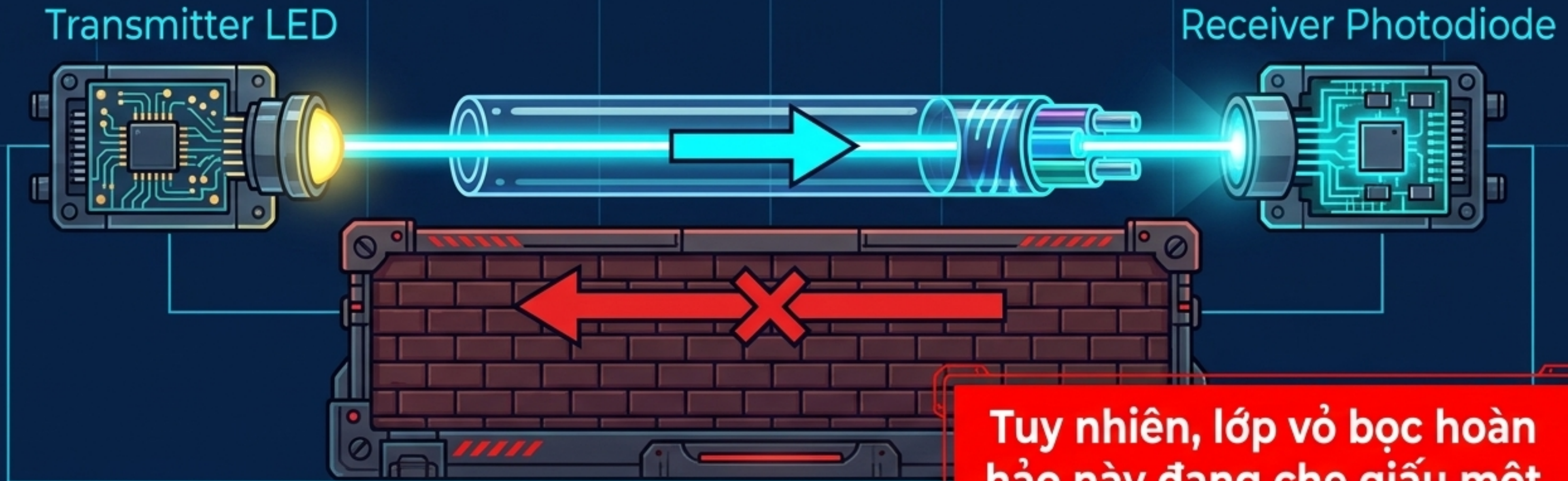
Chi phí vận hành thủ công khổng lồ.



Nguy cơ lây nhiễm chéo chí mạng qua thiết bị ngoại vi (USB) – Con đường kinh điển của mã độc Stuxnet phá hủy hệ thống hạt nhân.

DATA DIODE RA ĐỜI: KỲ VỌNG VỀ TIÊU CHUẨN VÀNG

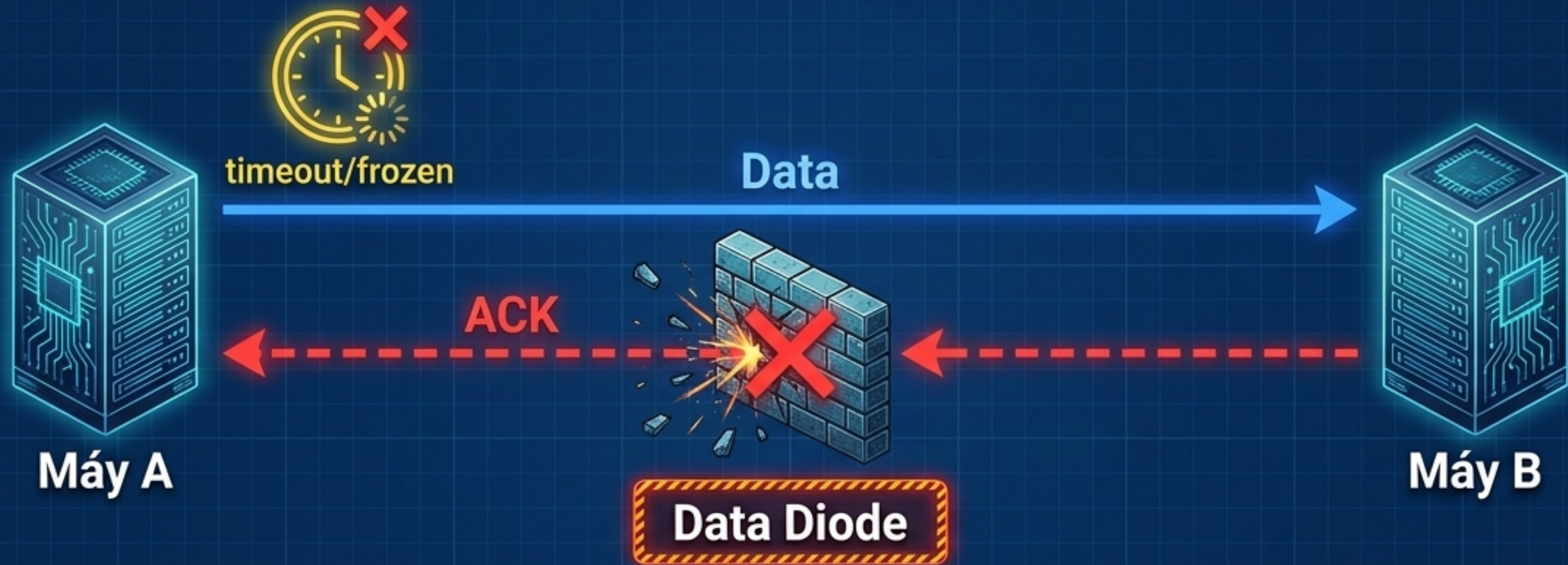
Giải pháp thay thế Air Gap dựa trên nguyên lý vật lý một chiều:
Chỉ cho phép dữ liệu đi vào (hoặc ra) qua cáp quang.



Tuy nhiên, lớp vỏ bọc hoàn hảo này đang che giấu một "ảo ảnh" chết người...

BẢN CHẤT ẢO ẢNH: “MÙ” TRƯỚC GIAO THỨC HIỆN ĐẠI

Các giao thức cốt lõi (TCP/IP) bắt buộc phải có cơ chế phản hồi hai chiều (gói tin ACK).



Data Diode chặn cứng chiều ngược lại. Hậu quả: Đẩy file 'mù quáng', rút gói tin không cảnh báo, tê liệt hoàn toàn các ứng dụng hiện đại.

4 NÚT THẮT CHÍ MẠNG CỦA DATA DIODE



1. Hiệu quả kinh tế cực thấp

Bắt buộc duy trì 2 hệ thống SOC biệt lập.
Chi phí bản quyền đắt đỏ cho từng giao thức.



2. Vận hành tồi tệ

Không hỗ trợ Call API, REST API.
Không thể quản trị máy chủ từ xa.



3. Lệ thuộc công nghệ

Lệ thuộc hoàn toàn vào các Proxy chuyển đổi giao thức đắt đỏ của hãng sản xuất.

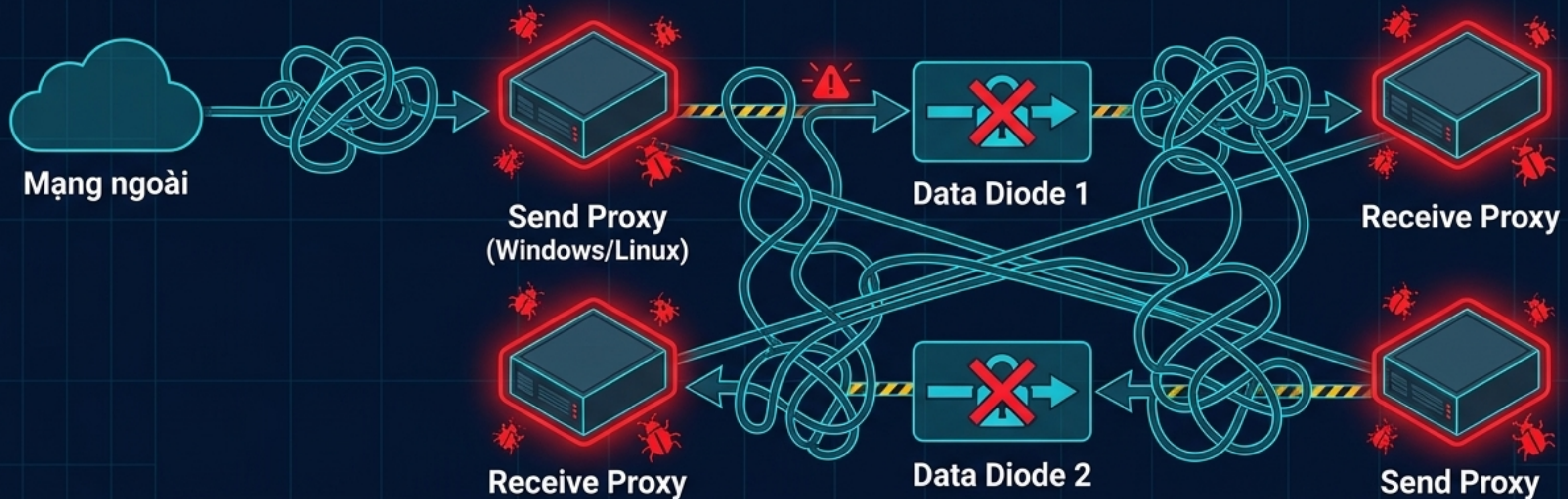


4. Tuổi thọ phần cứng ngắn

Cơ chế đẩy file mù quáng ép máy chủ ghi/đọc liên tục lên ổ cứng, gây hỏng hóc vật lý nhanh chóng.

CƠ ÁC MỘNG: ĐỒNG BỘ 2 CHIỀU BẰNG ‘PAIRED DIODES’

Để truyền 2 chiều, tổ chức phải ghép đôi ngược chiều và dùng vô số Proxy chạy HĐH thông dụng (Linux/Windows) để giả lập tín hiệu ACK.



Lỗi hỏng HĐH của Proxy mở ra bề mặt tấn công khổng lồ.
Ý nghĩa “cách ly vật lý” ban đầu hoàn toàn bị phá hỏng.

SECLAB SECURE XCHANGE NETWORK (SXN)

SỰ DỊCH CHUYỂN MÔ HÌNH: CÁCH LY ĐIỆN TỬ

Sẵn sàng tương thích tuyệt đối với TCP/IP nhưng KHÔNG duy trì kết nối mạng trực tiếp.

Xóa bỏ ảo ảnh vật lý thô sơ. Tương lai thuộc về kiến trúc bề gãy không gian mạng bằng phần cứng vi mạch tinh vi.

TRỤ CỘT 1: BẰNG GỖ GIAO THỨC TRIỆT ĐỂ (PROTOCOL BREAKING)

Hủy bỏ 100% vỏ giao thức gốc (L1-L4) nơi ẩn náu của 99% mã độc.



**Triệt tiêu hoàn toàn nguy cơ từ TCP SYN Flooding và các lỗi hổng IPnet.
Không một gói tin gốc nào có thể xuyên qua ranh giới.**

TRỤ CỘT 2: KIẾN TRÚC TƯỜNG CHẮN KÉP (DUAL-BARRIER)

3 bo mạch FPGA hoạt động hoàn toàn độc lập, không chia sẻ bộ nhớ, không dùng chung xung nhịp.

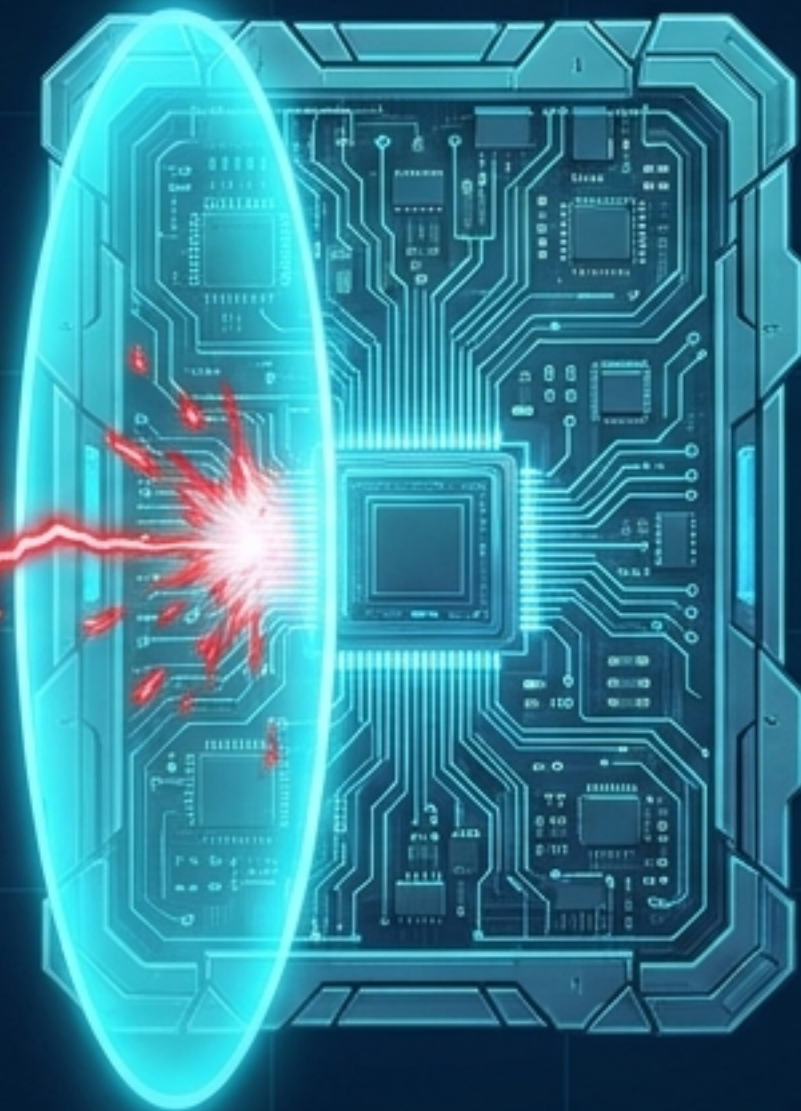
[GATE A]



Độc lập
Xung nhịp

Độc lập
Bộ nhớ

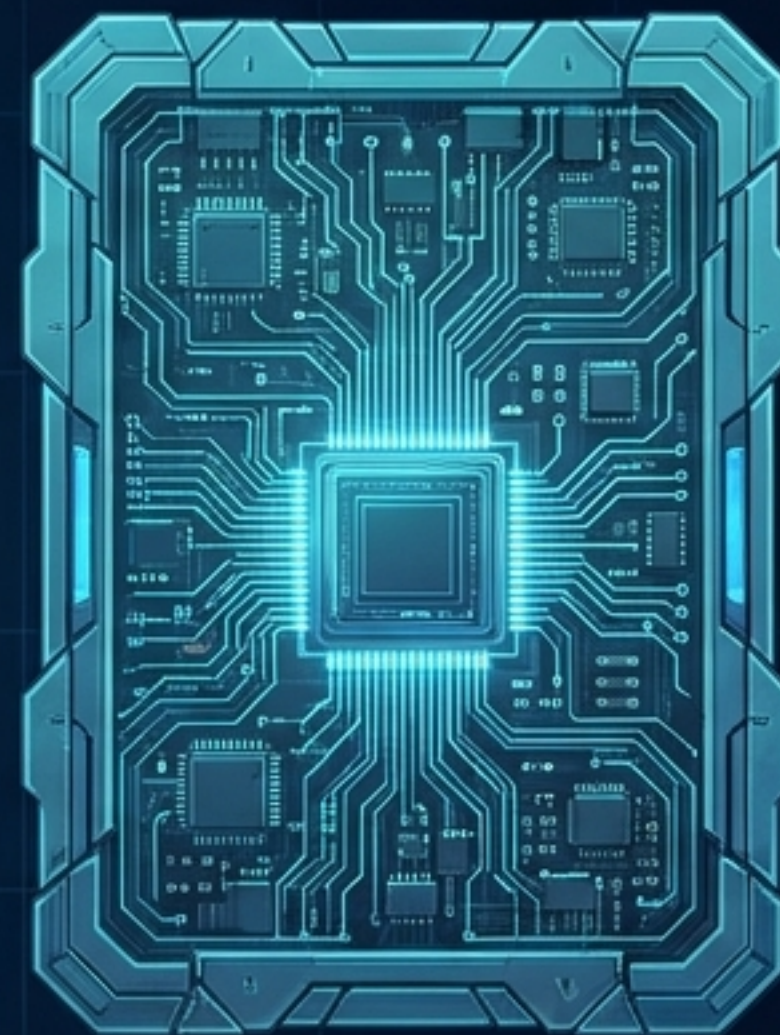
[CORE]



Độc lập
Xung nhịp

Độc lập
Bộ nhớ

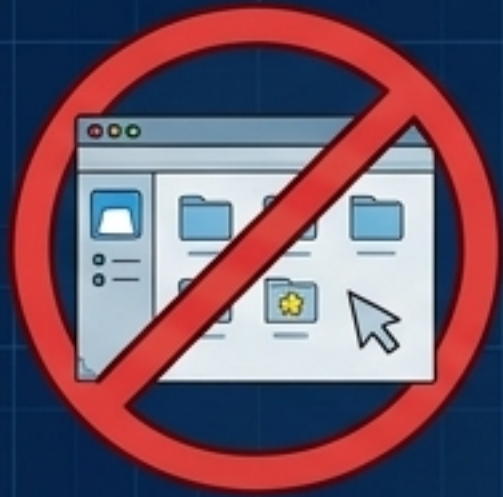
[GATE B]



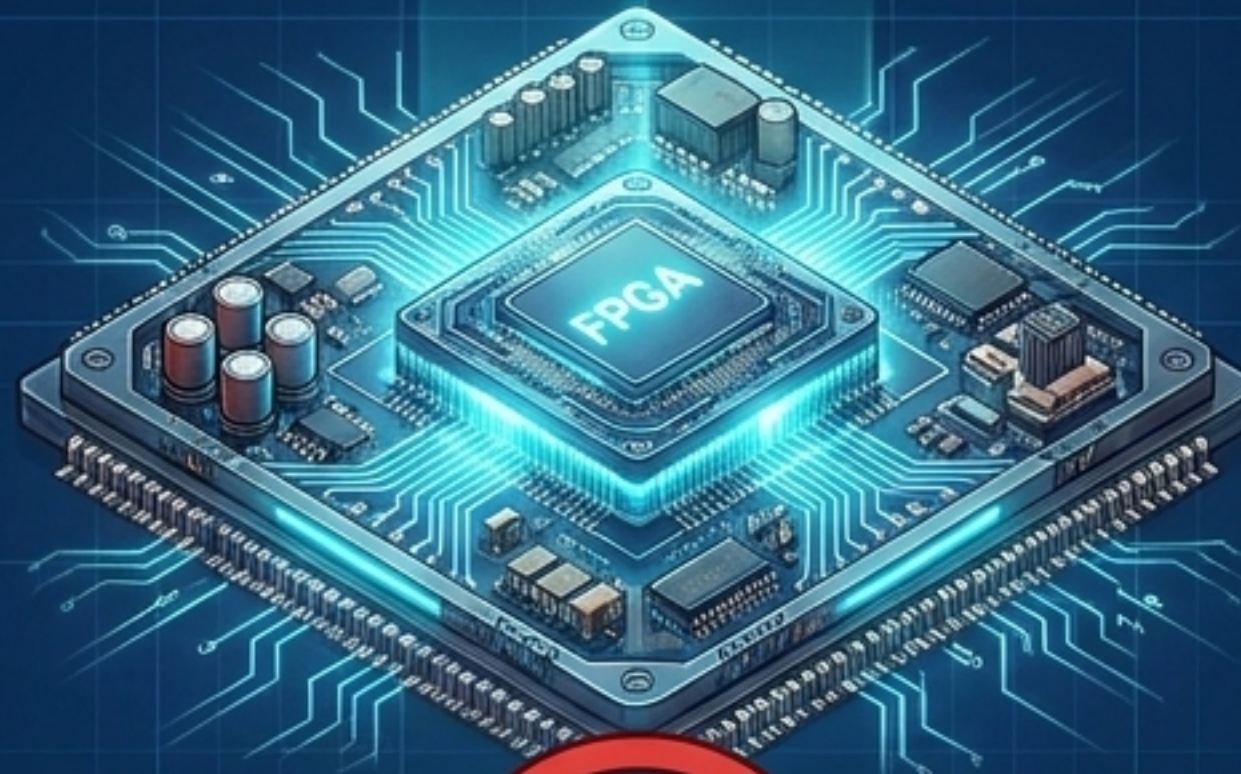
Kể cả khi Gate A bị chiếm quyền kiểm soát hoàn toàn, cuộc tấn công bị chặn đứng tuyệt đối tại vi mạch CORE vật lý.

TRỤ CỘT 3: LỖ VI MẠCH “ZERO OS / ZERO RUNTIME”

Trái tim hệ thống được lập trình cứng (Burnt FPGA) - không có môi trường thực thi lệnh.



NO Operating System
(Không Hệ điều hành)



NO Routing Table
(Không bảng định tuyến)



NO Software Execution
(Không thực thi phần mềm)

**Miễn nhiệm 100% trước mọi lỗ hổng Zero-day,
mã độc cấp hệ thống, và lỗi tràn bộ đệm (buffer overflow).**

SỨC MẠNH VẬN HÀNH THỜI GIAN THỰC

Hiệu năng phần cứng đỉnh cao, đáp ứng hạ tầng quy mô lớn. Tương thích hoàn hảo các giao thức OT/IT hiện đại mà không cần Proxy.



12,800

Kết nối đồng thời

10Gb SFP+

Băng thông siêu tốc

Call API

REST API

HTTPS

SQL

RDP

SSH

SCADA/PLC

SO SÁNH ĐỐI SÁNH KỸ THUẬT TRỰC QUAN

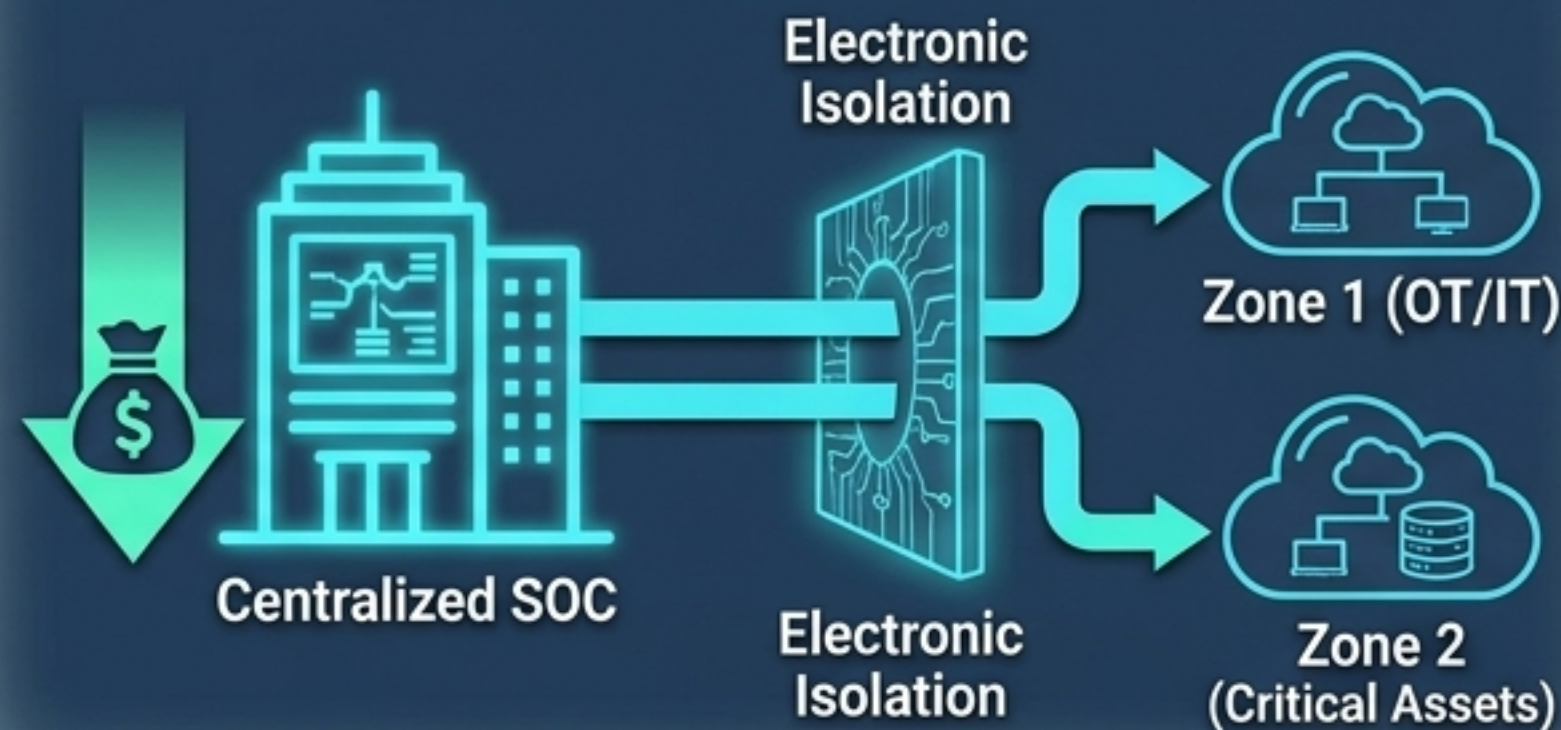
 Tiêu chí	FIREWALL	DATA DIODE	SECLAB SXN
Bảo mật	● Lọc phần mềm	● 1 chiều vật lý	● Cách ly điện tử 2 lớp
OS tại lõi	● Có OS	● Proxy có OS	● ZERO OS
Truyền 2 chiều	● Nguy cơ cao	● Mù / Lỗi proxy	● Hoàn hảo & An toàn
Xử lý gói tin	● Giữ nguyên	● Đẩy mù UDP	● Bẻ gãy & Tái tạo FPGA
Độ trễ	● Thấp	● Rất cao	● Cực thấp $\leq 1\text{ms}$

BÀI TOÁN KINH TẾ & TỐI ƯU HÓA HẠ TẦNG

Before - Data Diode



After - Seclab SXN



- **Tối ưu SOC:** Hợp nhất hệ thống giám sát an ninh về 1 SOC duy nhất, loại bỏ chi phí duy trì các 'hòn đảo' bảo mật. Zero-Maintenance.
- **Bảo vệ hệ thống di sản (Legacy):** Chốt chặn cứng bảo vệ tuyệt đối các hệ thống SCADA/PLC đời cũ chưa vá lỗi, không cần cài đặt agent.

BẢO CHỨNG BỞI CÁC TIÊU CHUẨN KHẮT KHE NHẤT THẾ GIỚI

Đạt chứng chỉ ANSSI CSPN hiếm hoi cho cả phần cứng & firmware.



Khuyến dùng bởi Phòng thí nghiệm NNLQG Hoa Kỳ (NREL).
Được triển khai thực tế trong môi trường Hạt nhân Châu Âu và chuẩn NATO-restricted.

KIẾN TẠO HẠ TẦNG CHUYỂN ĐỔI SỐ AN TOÀN TUYỆT ĐỐI

“Sử dụng Data Diode cho hạ tầng hiện đại giống như xây con đường đất một chiều giữa các siêu đô thị thông minh.”

(Data Diode)

(Electronic Isolation)

Cách ly điện tử (Seclab SXN) là câu trả lời của tương lai: Phá vỡ giới hạn vật lý, cân bằng hoàn hảo giữa an ninh tuyệt đối và vận hành thời gian thực.