OT Network Segmentation: Planning, Implementation, and Validation

Tony Turner

ICS Village



FRENOS



Tony Turner

I do security stuff for over 25 years now

I build security products at **Frenos**

- Author, Instructor at SANS
- Security Architect to Critical Infrastructure
- defendics.org
- cyberinformedengineering.com

FRENOS

AGENDA SLIDE

AGENDA

1. Understanding OT Network Segmentation Fundamentals
2. Planning Your Segmentation Strategy
3. Implementation Approaches and Technologies
4. Validation and Testing Methods
5. Case Study and Lessons Learned



FRENOS

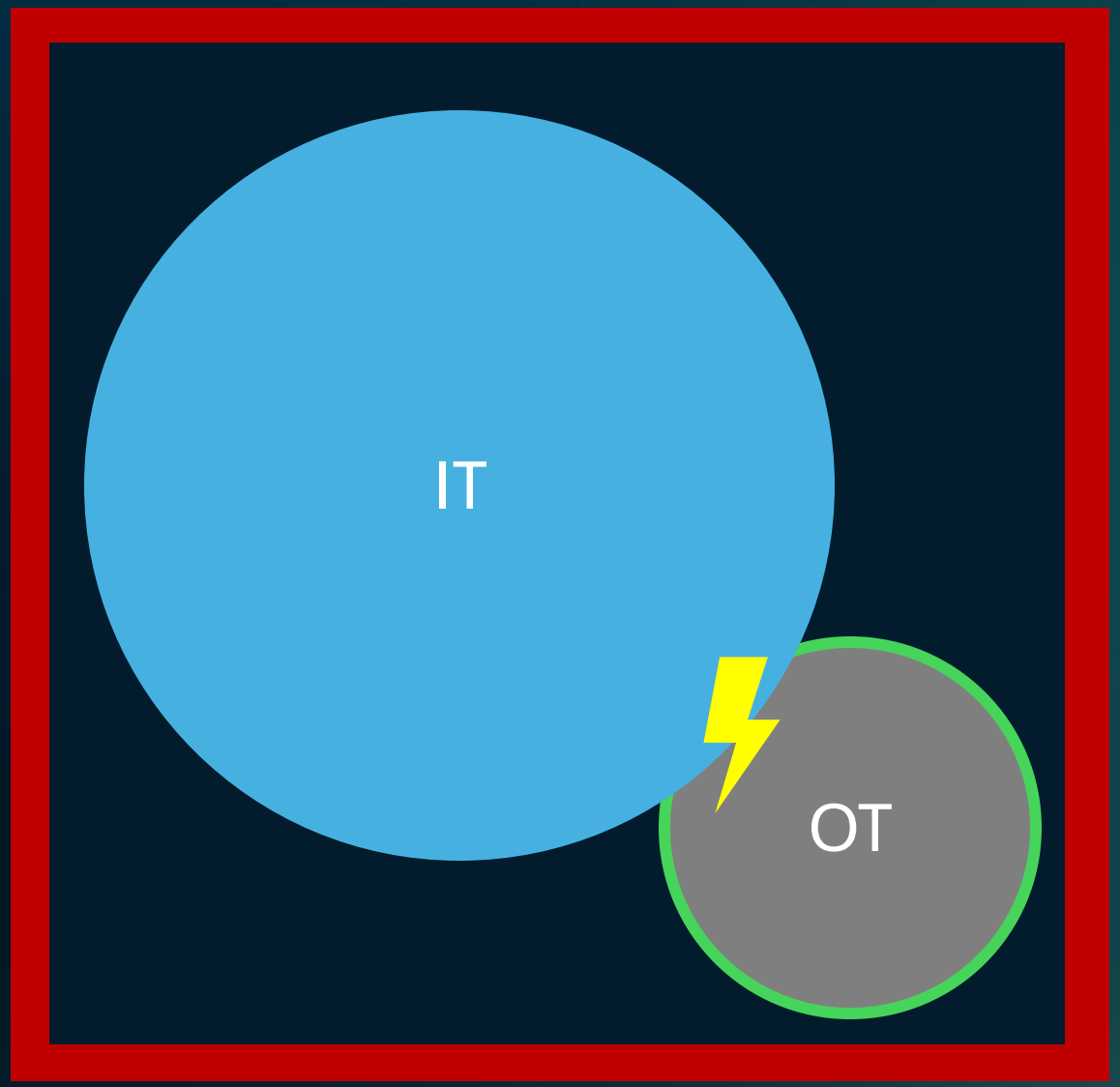
What is Segmentation?

Network segmentation is the practice of dividing a network into distinct subnetworks, each functioning as its own smaller network, with controlled communication paths between them.

(In other words, firewalls are just one way this is done)



FRENOS



IT-to-OT is Primary attack vector

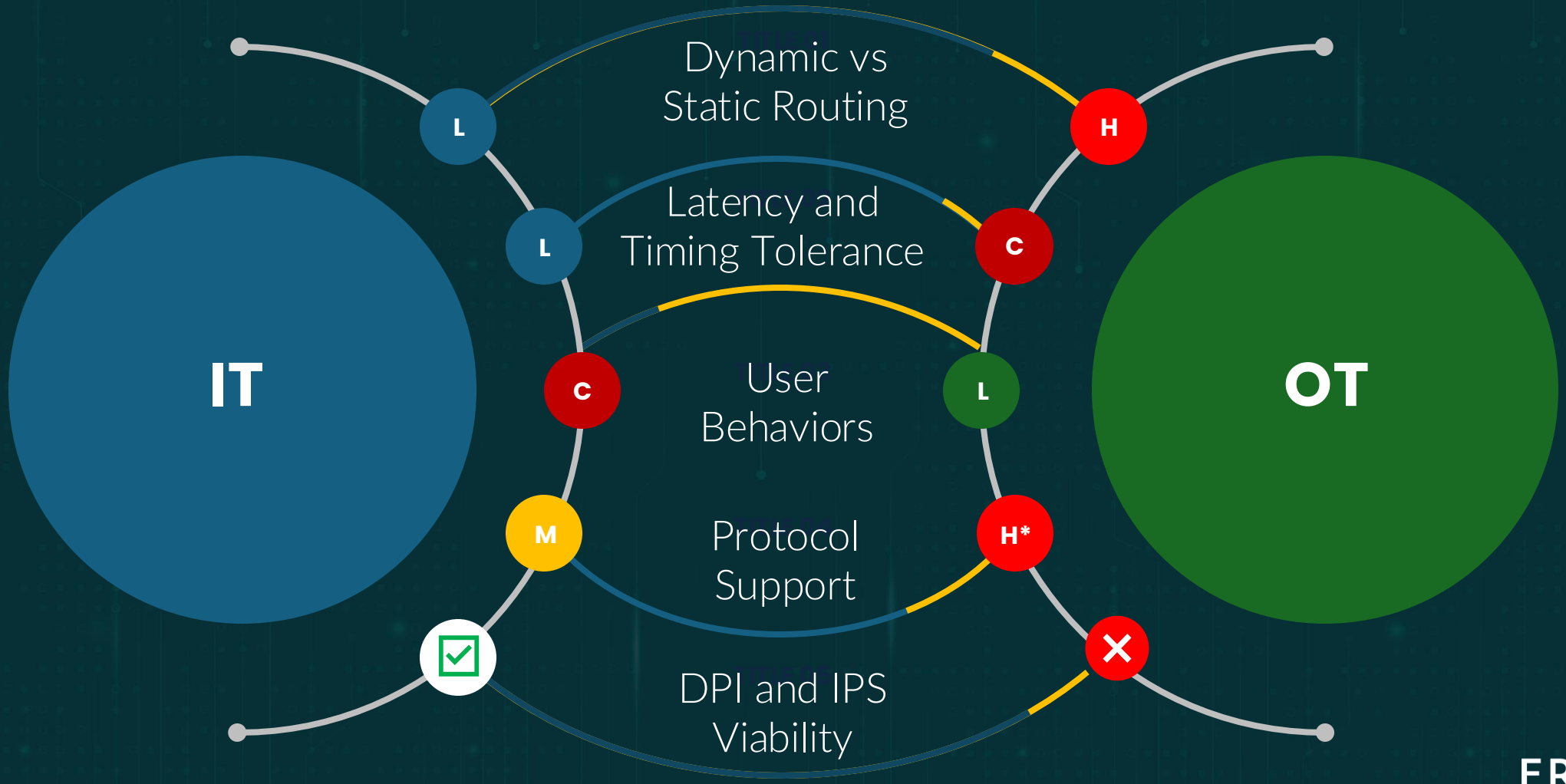
Why OT Network Segmentation Matters

- Vendor (hardening) challenges
- Network chokepoints
- OT Access
- OT Visibility

FRENOS

TWO-OPTION COMPARISON

Segmentation Differences



FRENOS

Reference Architecture

Purdue Architecture – not a security Architecture but useful for conversation

Here be Dragons!

Level 4 (IT Enterprise) to 5 (Internet / Cloud)

IT/OT DMZ

Level 3 – Control Center

Facility Segmentation

Level 2 - Facility

Level 2 - Facility

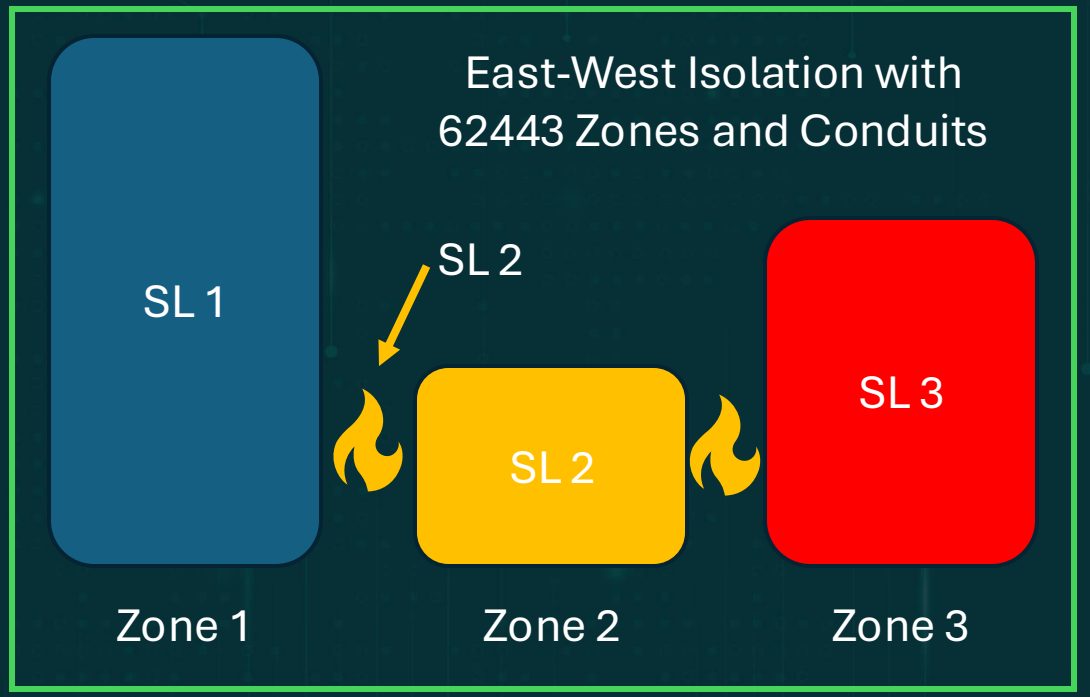
Level 1 - Subsystem

Level 1 - Subsystem

Level 0 - Process

Level 0 - Process

*Note Firewall zones are about trust, while 62443 zones are about common security requirements



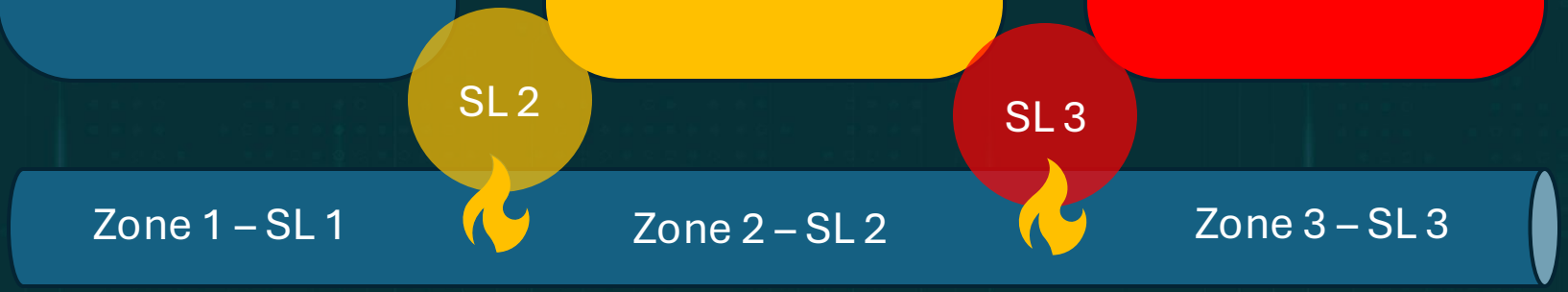
FRENOS

Zone Design Principles

- Enterprise data collection systems
- Historical trend databases
- Non-critical reporting servers
- Business intelligence applications
- Maintenance planning systems

- SCADA/HMI operator workstations
- Production management systems
- Batch control servers
- Historian collection points
- Engineering workstations

- Safety instrumented systems
- Critical control PLCs
- Real-time controllers
- Emergency shutdown systems
- Core process automation controllers



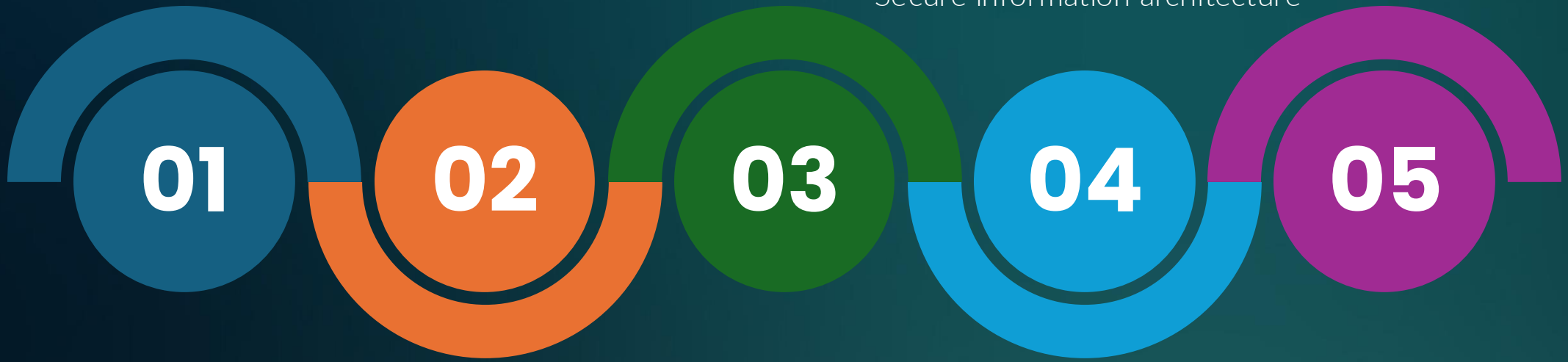
Function-Based Boundaries
Group systems with similar security needs

Controlled Conduits
Define explicit communication paths

Risk-Driven Security Levels
SL determines boundary controls

FRENOS

Planning Process



INVENTORY

Walkdowns
CMDB
Compliance data
INSM Sensors

COMMUNICATION MAPPING

Functional Requirements
Reliability and Safety
Network characteristics

RISK ASSESSMENT

Threat-informed scenarios
Security Requirements
Consequence oriented

ZONE DESIGN

Minimal communication paths
Resilient Layered Defense
Secure information architecture

CONTROL SELECTION

Firewall vs diode vs “air-gap”
DPI support
Operational impacts
Validation

FRENOS

Technology Selection Options



NGFW

Enforces boundary with protocol awareness

Zone transitions, protocol filtering



VLAN

Logical separation within infrastructure

Initial segmentation, same physical network



ROUTER ACL

Basic filtering at network perimeter

First line defense, IP/port filtering



DATA DIODE

One-way information flow

Critical safety systems, highest security

FRENOS

Segmentation Validation Methods

	When to Use	Advantage	Considerations
Rule Review	Initial validation	Non-disruptive Compliance	Static testing only No scenario modeling
Digital Twin Simulation	Initial and Continuous	Zero operation risk Threat scenarios Continuous	Requires frequent model updates
Passive Monitoring	Continuous Validation	Real-time Actual traffic flows	Reactive only Potential blind spots
Active Testing	Periodic verification	Actual system behaviors	Does not scale Creates ops risk Disruptive



FRENOS

Manufacturing Case Study

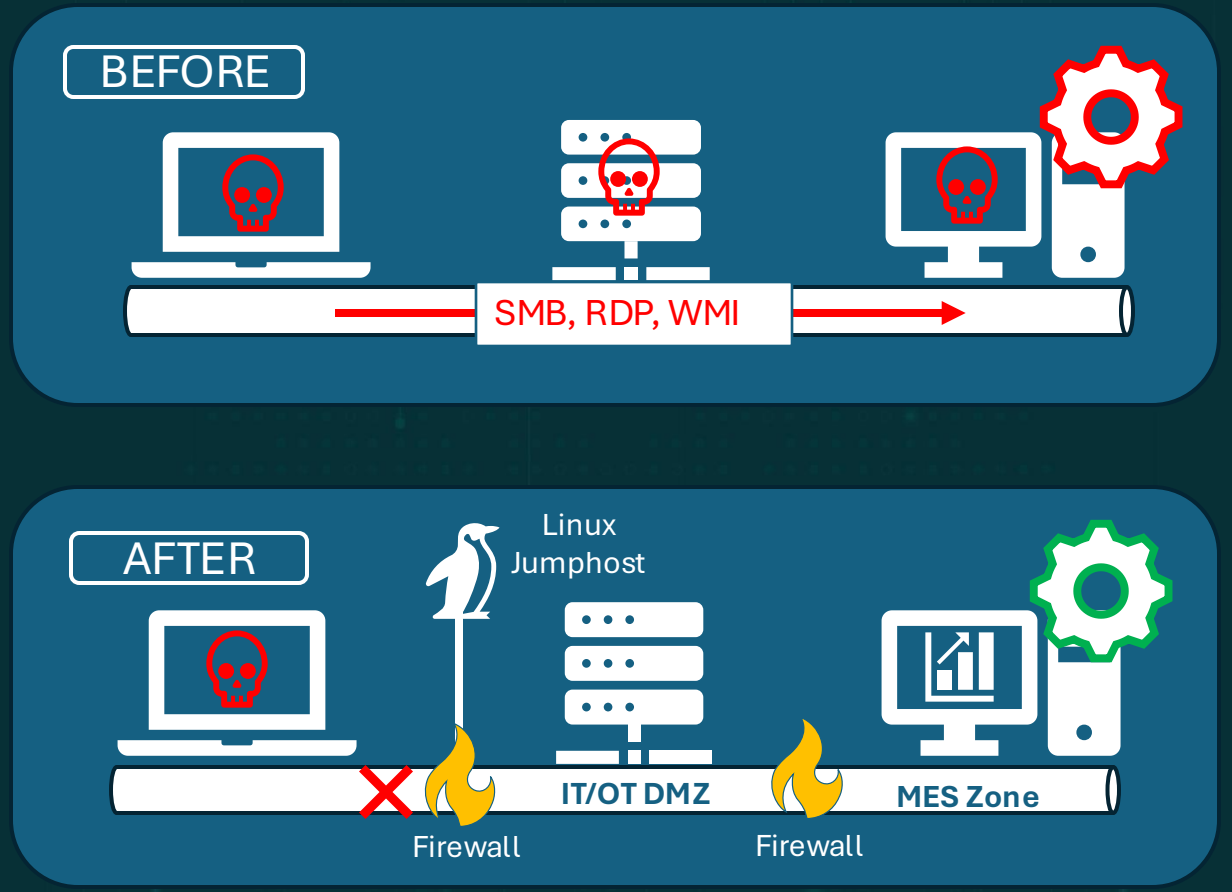
Industry: Automotive Parts Manufacturing

Problem: Architected as a flat network, suffered a ransomware attack that spread from corporate email to production HMIs, halting three production lines for 72 hours.

Solution: OT network segmentation with strict controls blocking SMB, RDP, and WMI traffic between zones and Linux jumphost for secure remote access

Outcome: A subsequent corporate ransomware infection was contained to IT systems. OT Cyber isolated critical systems by disabling IT interface.

Production continued uninterrupted, avoiding an estimated $450,000 in losses and validating the segmentation investment.



FRENOS

Common Segmentation Pitfalls

Static rules without regular review	Change Management, Automation
Too many exceptions weaken segmentation	Business justification, Risk-based Audit
Unaddressed protocols create gaps	Inventory and Test, Allow-list
No visibility into segmentation effectiveness	Log, Monitor, Audit tooling
Fear and lack of understanding lead to loose config	Assess, Incremental Improvement

FRENOS

Key Takeaways

Know what you are protecting and why

Define Functional and Security Requirements

Isolate Critical Systems and Manage Access

Assess and Validate Continuously!



FRENOS

FRENOS

THANK YOU!

Tony Turner
VP, Product

https://frenos.io

