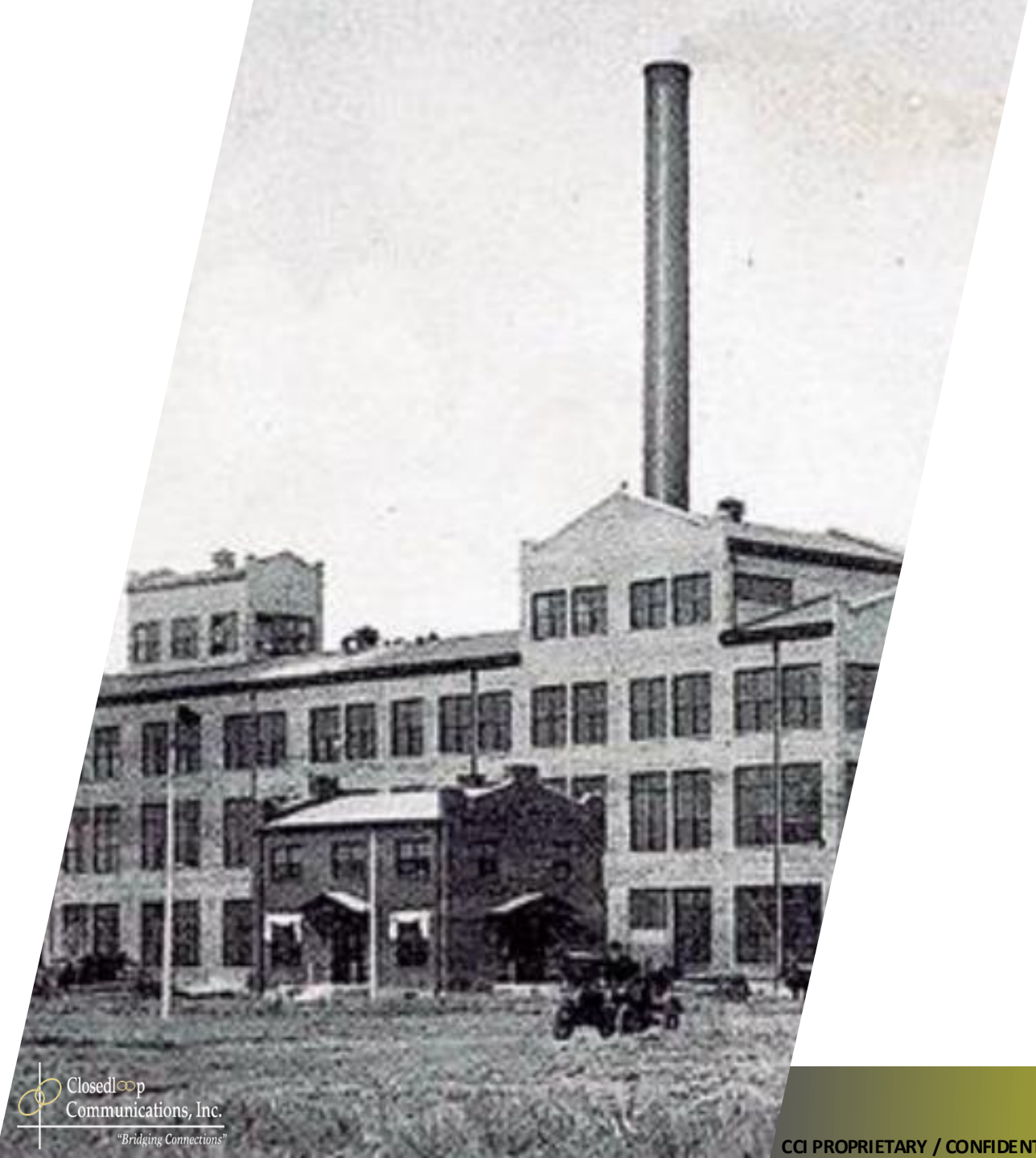
ZERO TRUST – OPTIMIZING IT INTEGRATION INTO OT ENVIRONMENTS

Closedloop Communications, Inc.
"Bridging Connections"



SIGNS OF OT

MODULAR DIGITAL CONTROLLER, 1969

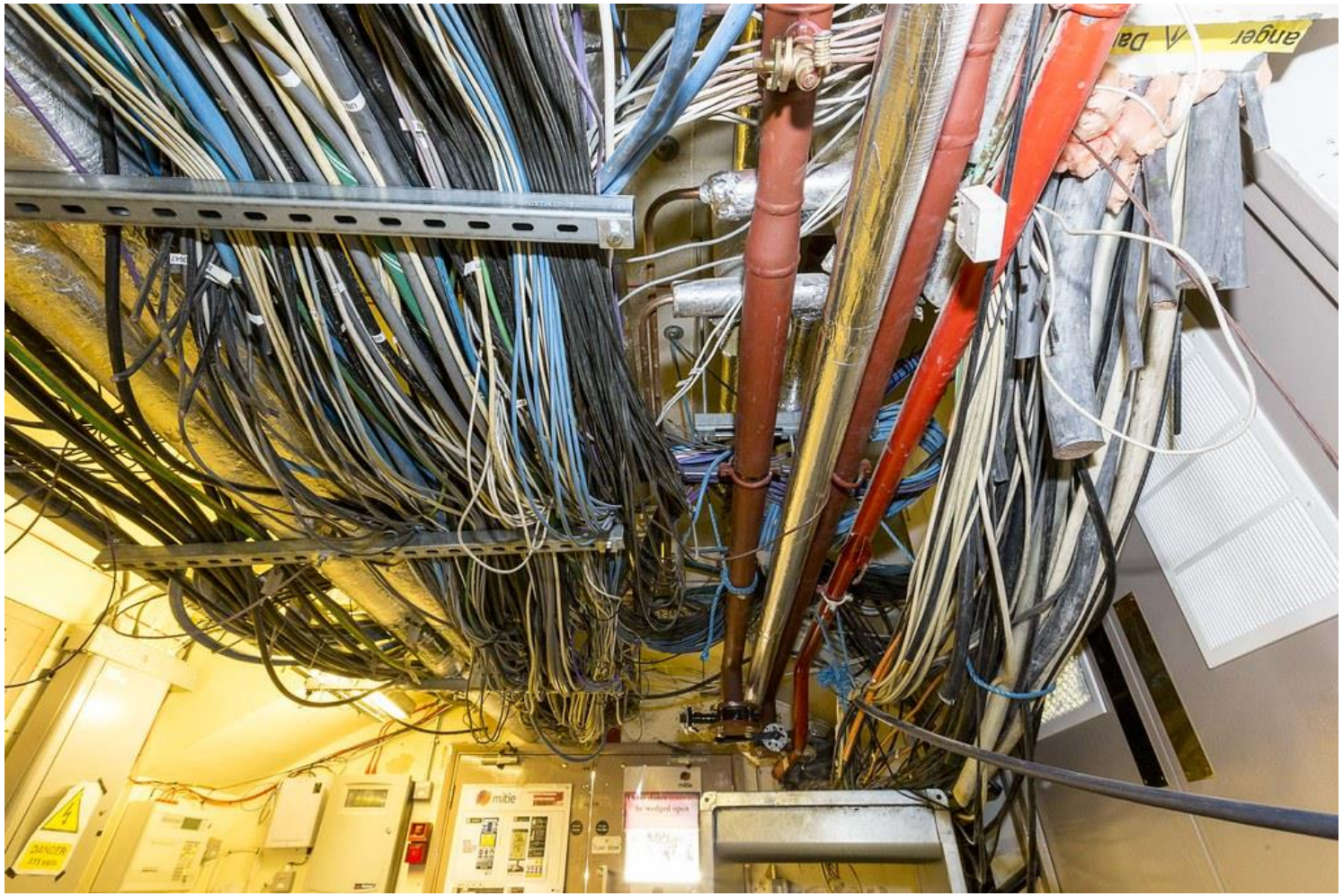
GARTNER ENERGY AND UTILITIES IT SUMMIT, 2006

ISA-99.00.01, “SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS”, 2007

Closedloop Communications, Inc.
“Bridging Connections”

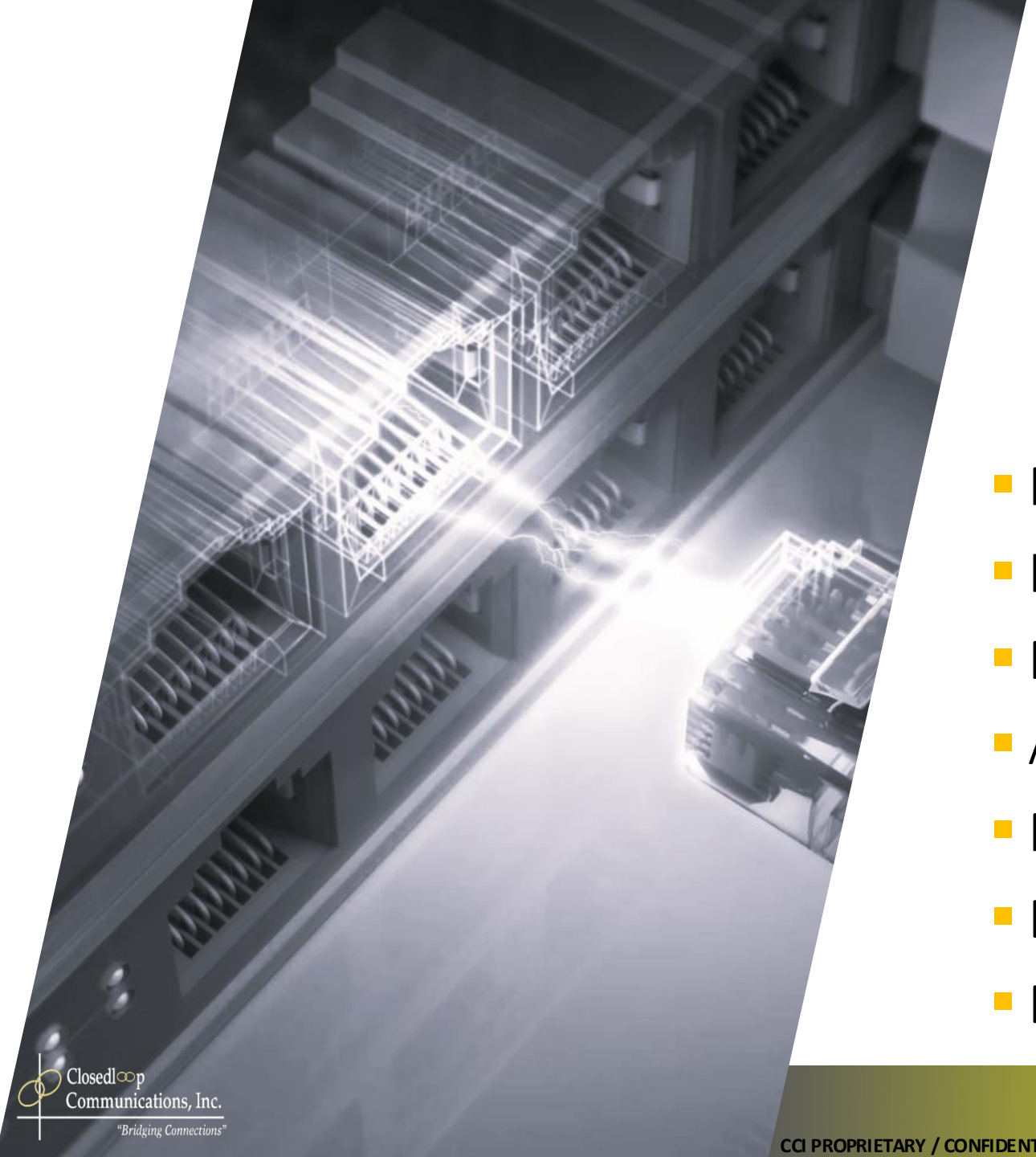
WHY CRITICAL INFRASTRUCTURE WANTS ETHERNET

- Interleaved communications
- Easier troubleshooting
- Flexible topologies
- Additional communication telemetry
- Faster communication
- Advanced access control and communication



TRADITIONAL ETHERNET BEHAVIOR

- Interoperable
- Distributed control
- Auto learning and dynamic address tables
- Broadcasting capability
- Implicit trust of packets
- Auto loop mitigation



INHERENT OT VULNERABILITIES OF TRADITIONAL ETHERNET

- Packet flooding
- Host spoofing
- Packet injection
- ARP poisoning and spoofing
- Network reconnaissance
- Distributed denial of service
- Ethernet management protocols

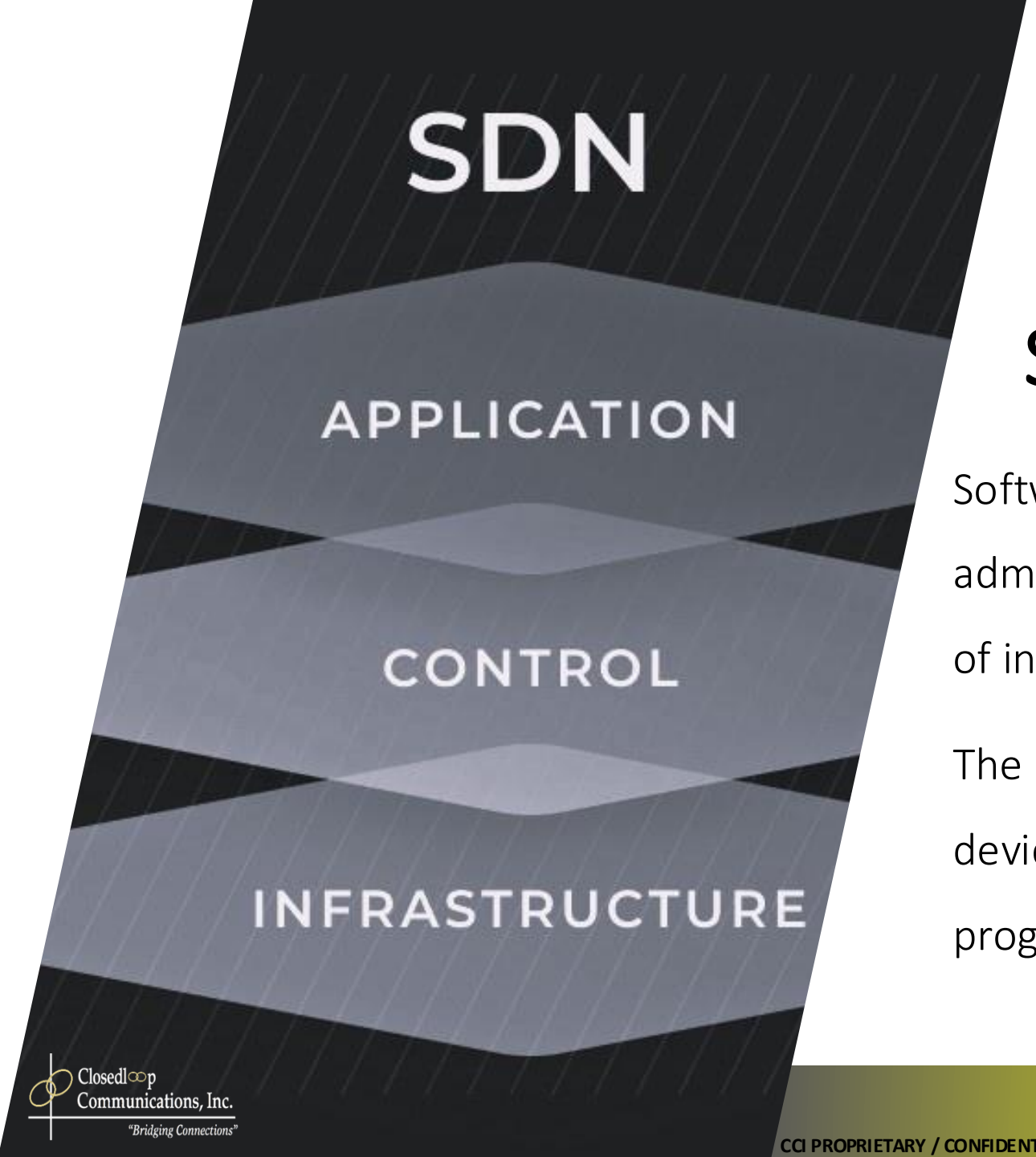
Closedloop Communications, Inc.
"Bridging Connections"

OTSDN - DEVELOPED IN COLLABORATION

Pacific Northwest NATIONAL LABORATORY

Sandia National Laboratories

TCIPG



SDN DEFINED

Software Defined Networking (SDN) is the centralized administration of the communications and forwarding of information in a packet-based switching network.

The control plane is abstracted from packet forwarding devices to a centralized controller that can then program and orchestrate network behavior.

Closedloop Communications, Inc.
"Bridging Connections"

SDN vs. OTSDN

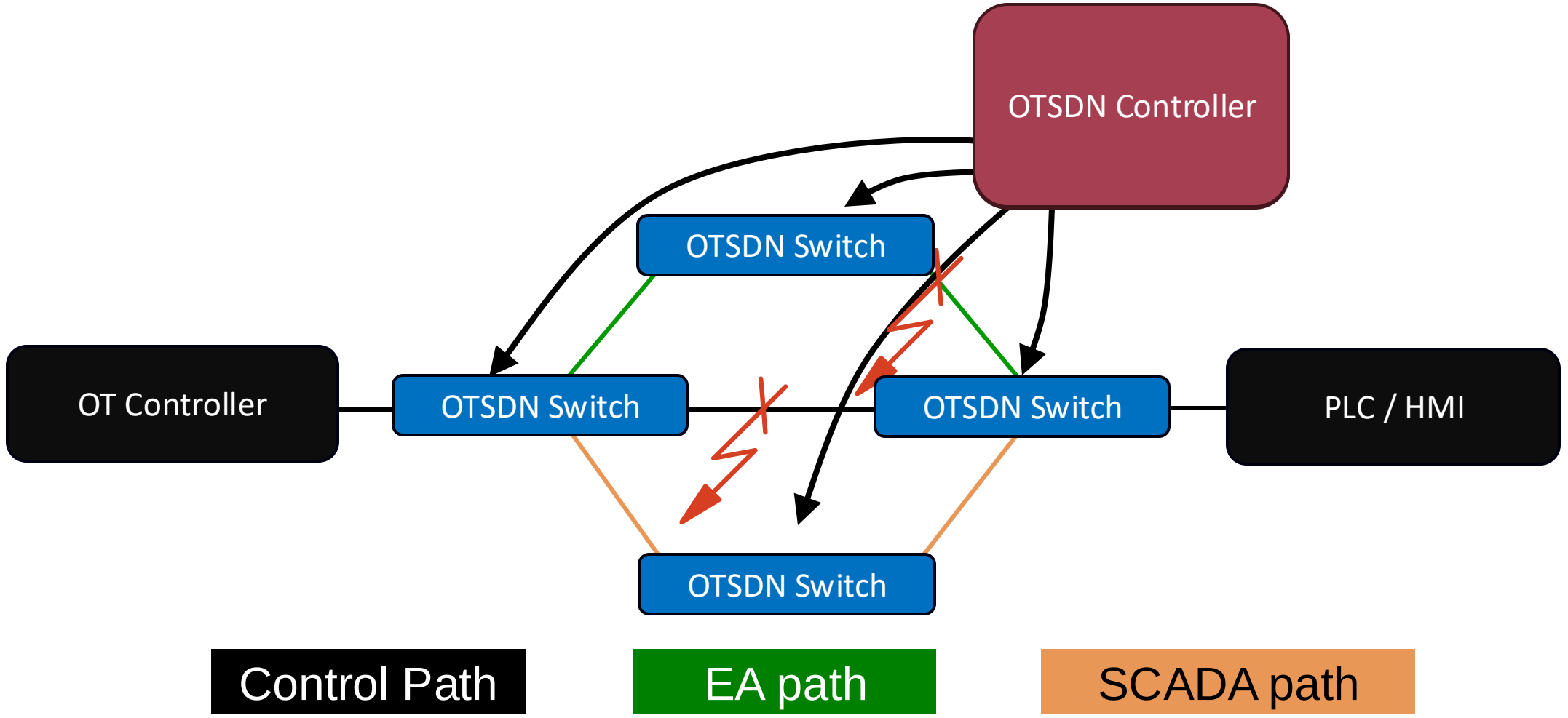
SDN

- Dynamic centralized packet learning and forwarding
- Fast network level configuration changes
- Automation of routine manual tasks
- Unified view of entire network, simplifying operations

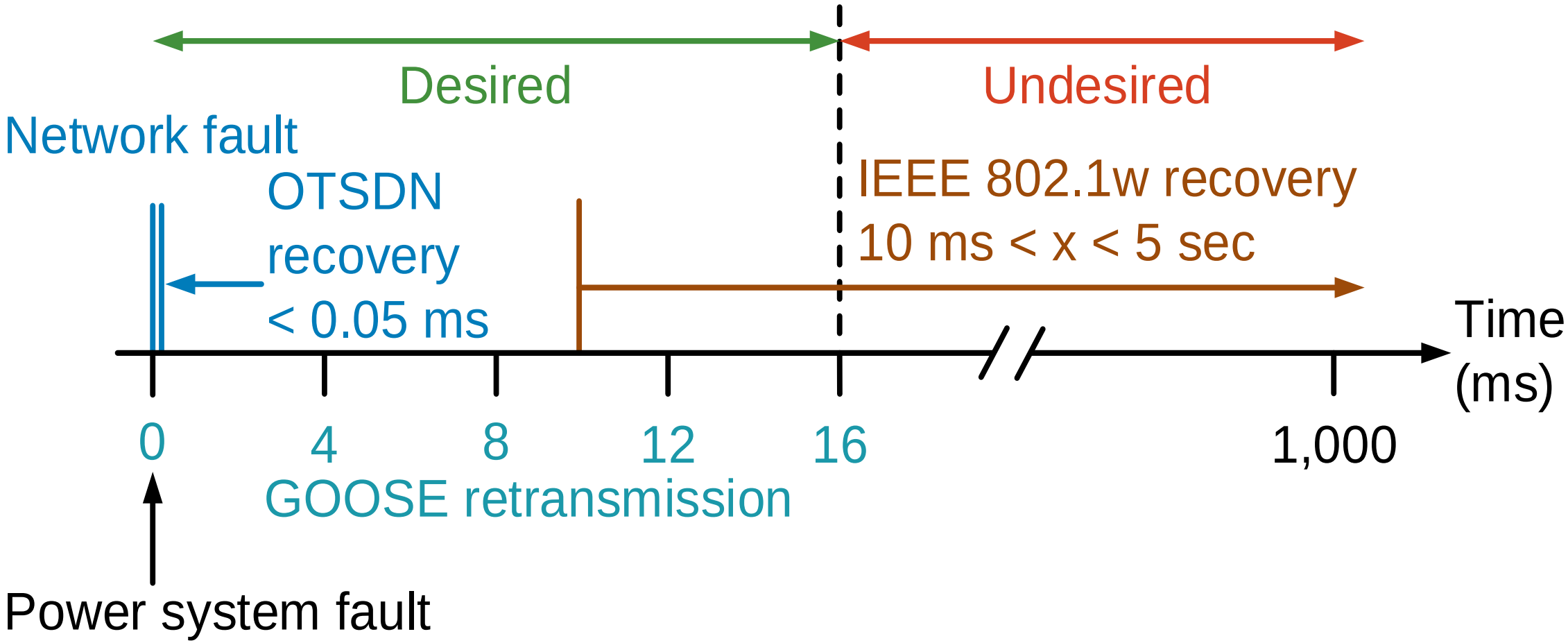
OTSDN

- Traffic engineered forwarding and failover
- Real-time failover recovery
- Deny-by-default forwarding and packet categorization
- Advanced baselines, network telemetry, and monitoring

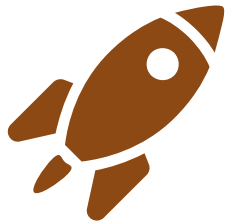
OTSDN OPERATION



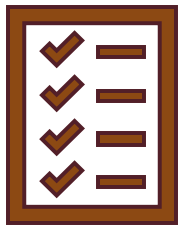
OTSDN REAL-TIME FAILOVER



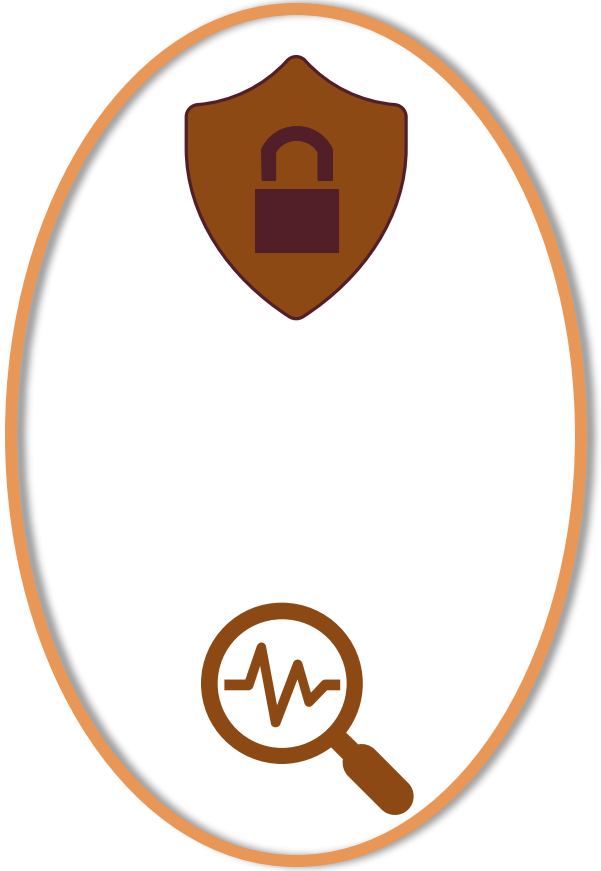
OTSDN BENEFITS



Performance and Function

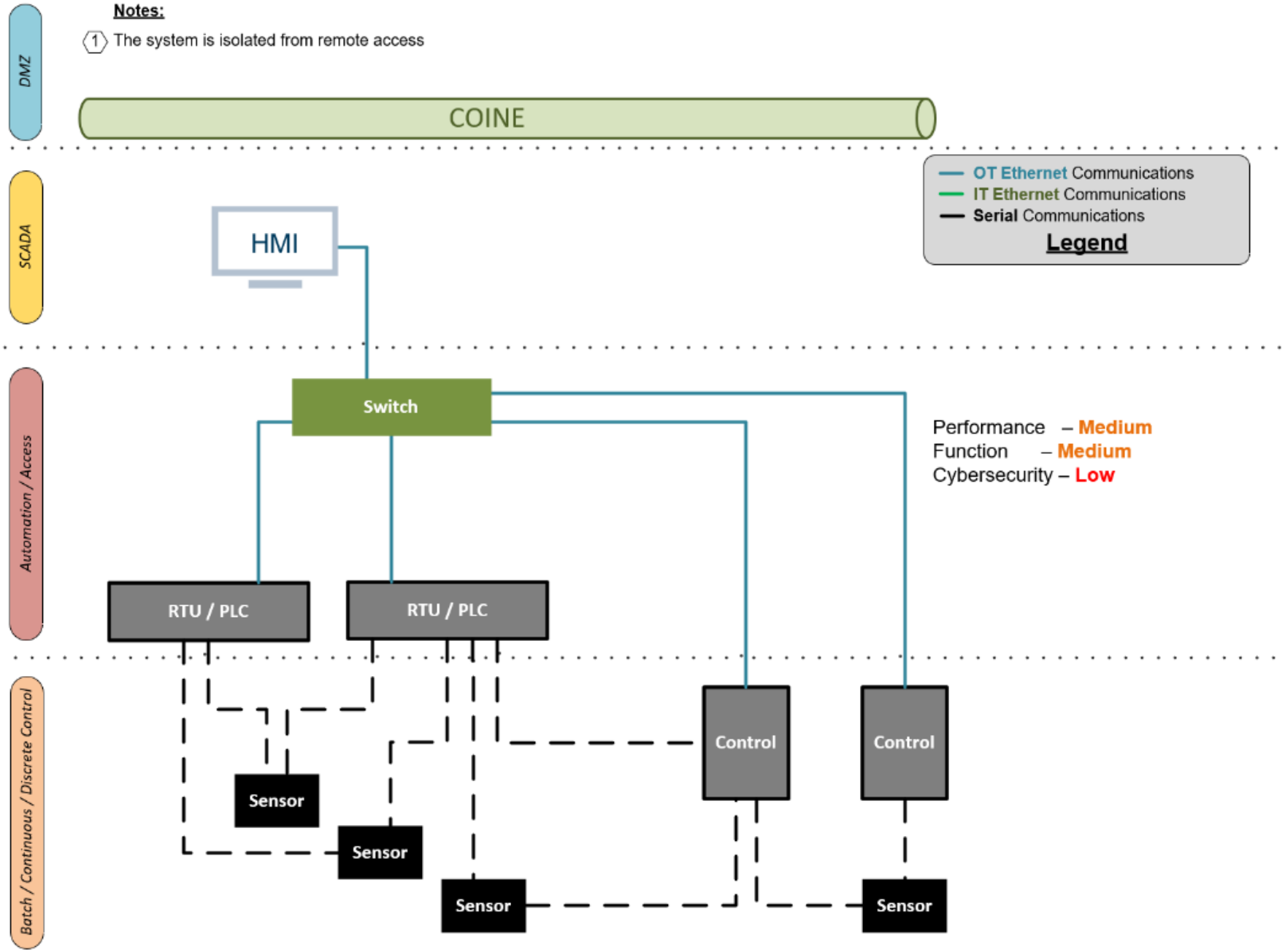


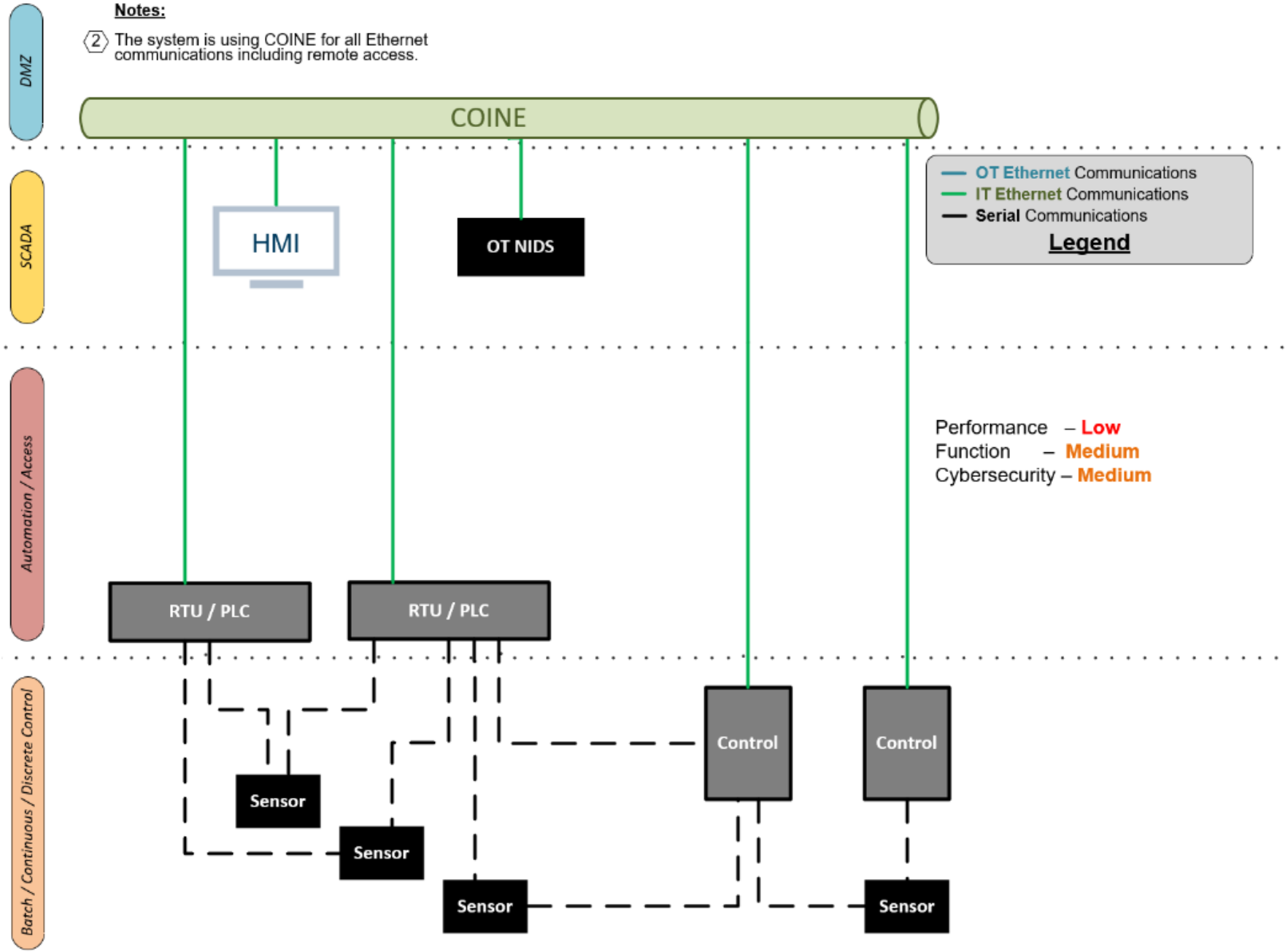
Engineered Compliance



Cybersecurity

Increased Awareness


Notes:
1 The system is isolated from remote access
DMZ
COINE
SCADA
HMI
OT Ethernet Communications
IT Ethernet Communications
Serial Communications
Legend
Switch
Automation / Access
Performance – Medium
Function – Medium
Cybersecurity – Low
RTU / PLC
RTU / PLC
Batch / Continuous / Discrete Control
Control
Control
Sensor
Sensor
Sensor
Sensor


Notes:
2 The system is using COINE for all Ethernet communications including remote access.
DMZ
COINE
SCADA
HMI
OT NIDS
OT Ethernet Communications
IT Ethernet Communications
Serial Communications
Legend
Automation / Access
Performance – Low
Function – Medium
Cybersecurity – Medium
RTU / PLC
RTU / PLC
Batch / Continuous / Discrete Control
Sensor
Sensor
Sensor
Control
Control
Sensor

IT TECHNOLOGY vs. OTSDN

Layer 2 Ethernet Switch

Layer 3 Ethernet Switch

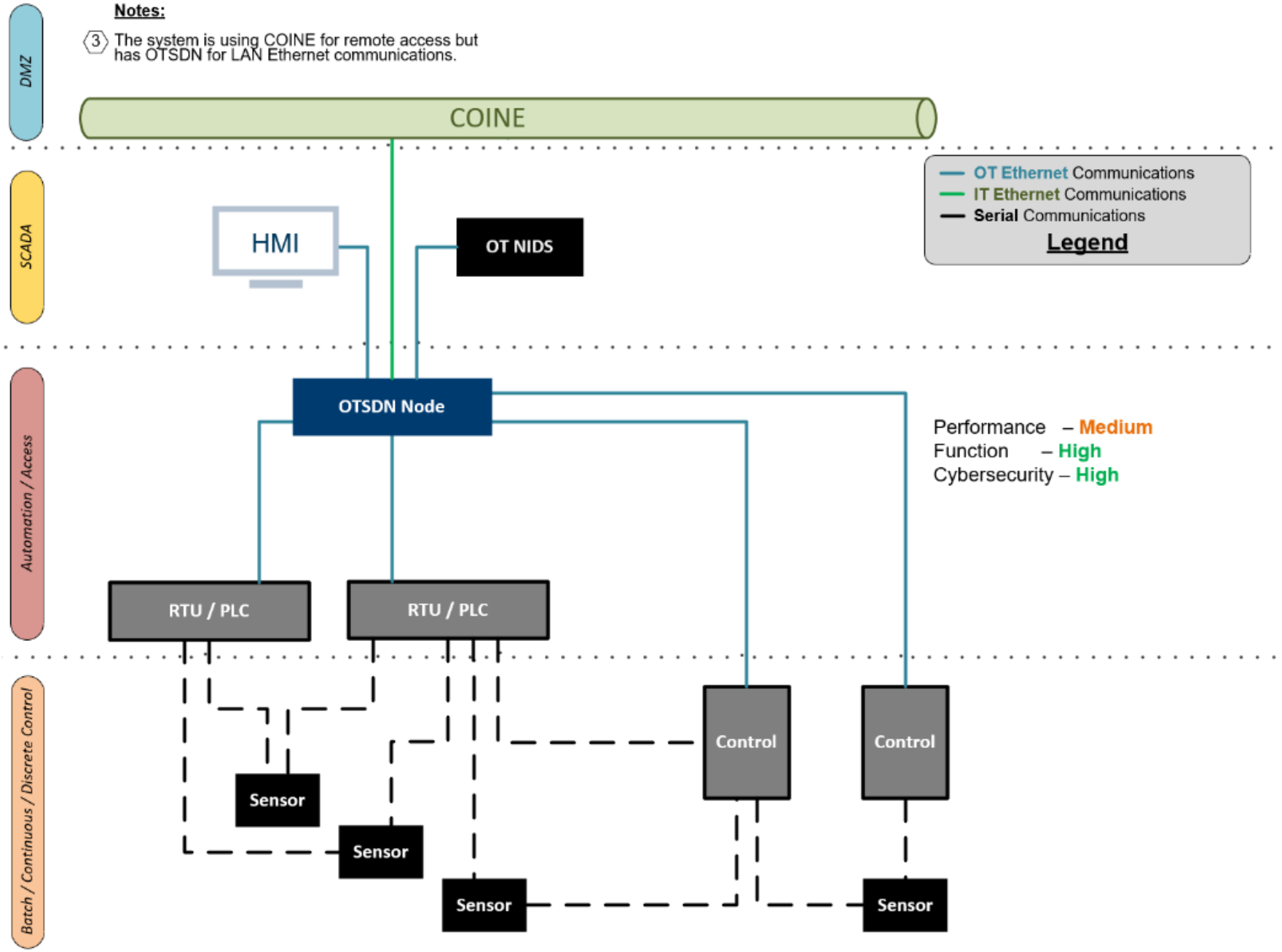
IP Router

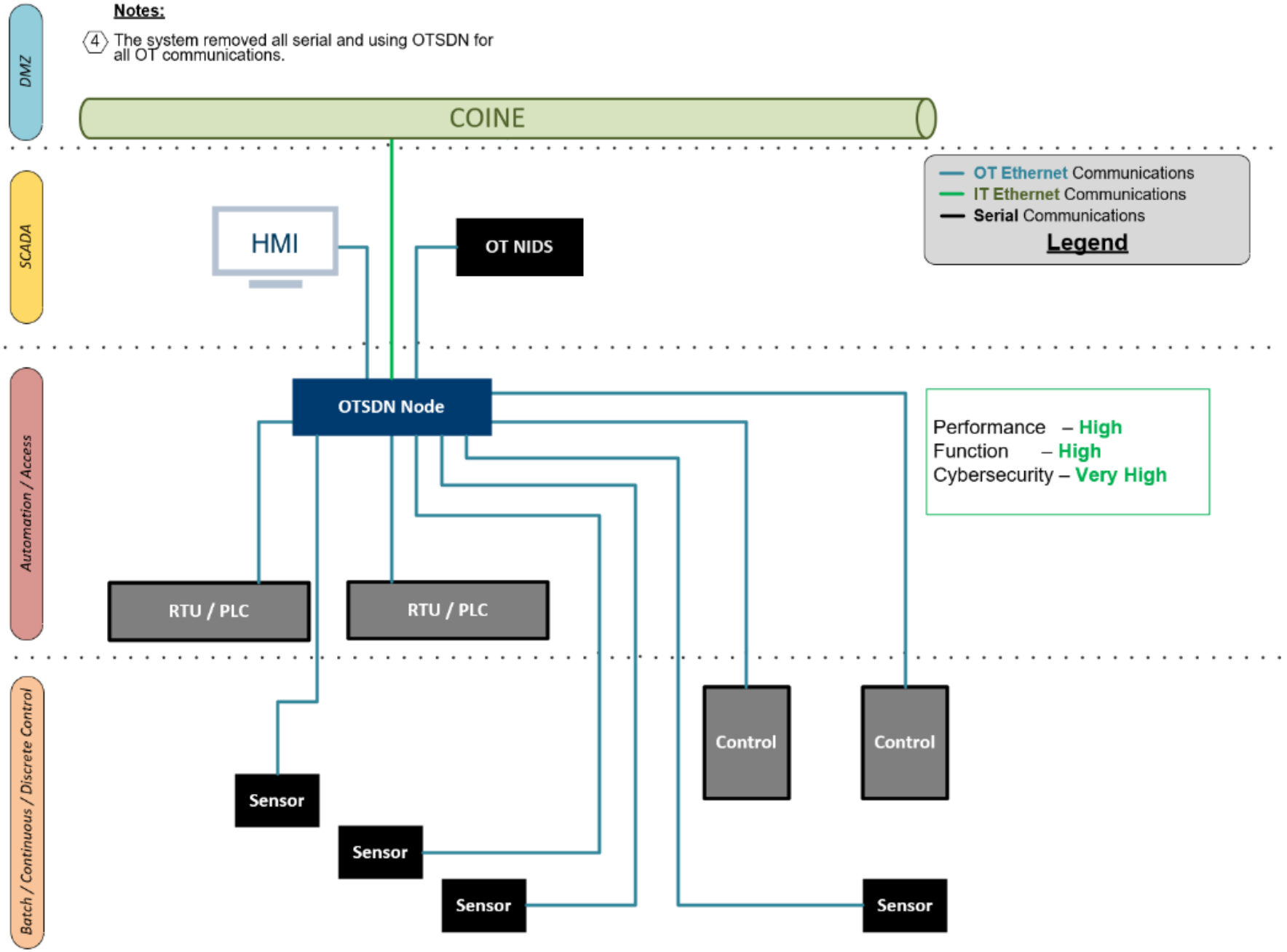
Firewall

} OTSDN

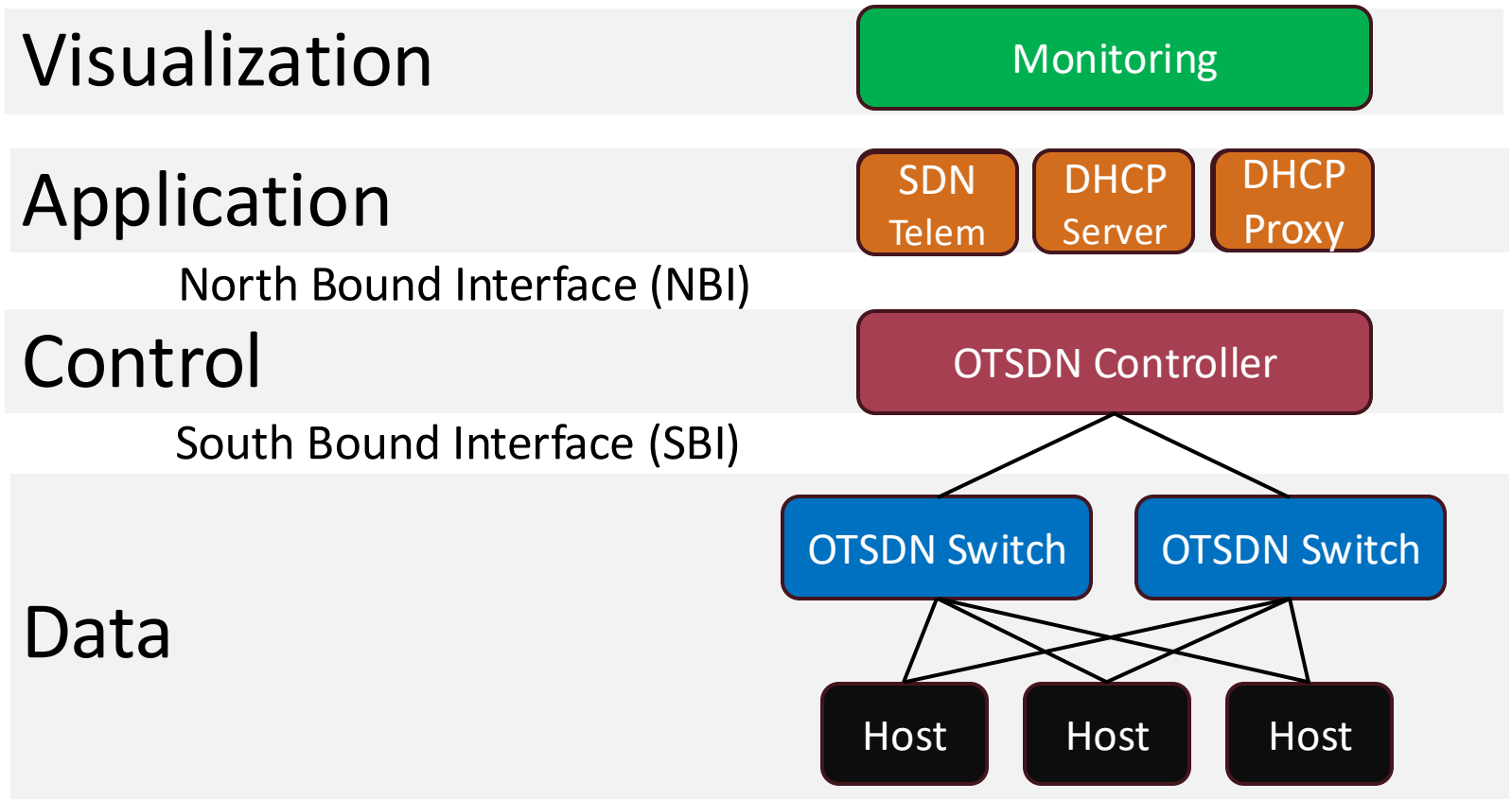
Next Generation Firewall = OTSDN + Next Generation IDS

VPN = OTSDN + RTU/PLC


Notes:
3 The system is using COINE for remote access but has OTSDN for LAN Ethernet communications.
DMZ
COINE
SCADA
HMI
OT NIDS
OT Ethernet Communications
IT Ethernet Communications
Serial Communications
Legend
Automation / Access
OTSDN Node
Performance – Medium
Function – High
Cybersecurity – High
RTU / PLC
RTU / PLC
Batch / Continuous / Discrete Control
Control
Control
Sensor
Sensor
Sensor
Sensor


Notes:
4 The system removed all serial and using OTSDN for all OT communications.
DMZ
COINE
SCADA
HMI
OT NIDS
OT Ethernet Communications
IT Ethernet Communications
Serial Communications
Legend
Automation / Access
OTSDN Node
Performance – High
Function – High
Cybersecurity – Very High
RTU / PLC
RTU / PLC
Batch / Continuous / Discrete Control
Control
Control
Sensor
Sensor
Sensor
Sensor

ZTA OTSDN A&E



- ZTA Specification & SRG
  - OTSDN Security Requirements
  - OTSDN Testing
- OT STIGs
- OTSDN IDS Functions
- OTSDN Applications

MEASURING ZT LEVEL OF MATURITY

- Select Security Controls that map to ZT Capabilities ZT Security Controls
- Map ZT Security Controls to ZTA Components (PE, PA, PEP, PIP, & OE)
- Develop ZTA Component Requirements ZTA Component SRG
- Establish Technology Requirements according to ZTA Component SRG
- Institute new OT ZT Capabilities (Protocol Break, Engineering Access Proxy)
- Generate ZTA STIG on OT System for Technology (OT SDN, RTAC, Blueframe)
- Produce ZT Roadmap (ZTMM) for ZTA Technology (OT SDN, RTAC, Blueframe)

OT ROAD MAP ZERO TRUST MATURITY & CAPABILITIES

Basic Level

- Data flows mapped
- Programmable network infrastructure
- Micro-segmentation with hop-by-hop communication verification
- Engineering access proxy

Intermediate Level

- Continuous diagnostics, policy rules, and monitoring
- Dynamic policy rules with threat intelligence input
- OT security information and event management
- OT network and system event log correlation
- Multifactor Authentication

Advanced Level

- Continuous authentication
- Contextual and granular permissions
- Micro-perimeter with hop-by-hop communication authentication
- Cybersecurity policy automation and orchestration

THANK YOU

Dennis Gammel

509.432.6216

gammel.d@closedloopcomm.com

www.closedloopcomm.com

Closedloop Communications, Inc.

"Bridging Connections"