Cisco live!

July 10-14, 2016 · Las Vegas, NV

Your Time Is Now

IoT Solutions - Connecting Oil and Gas Pipelines

Jason Greengrass, IOT Solution Architect

Rik Irons-Mclean, Oil & Gas and Energy Architecture Lead

BRKIOT-2109

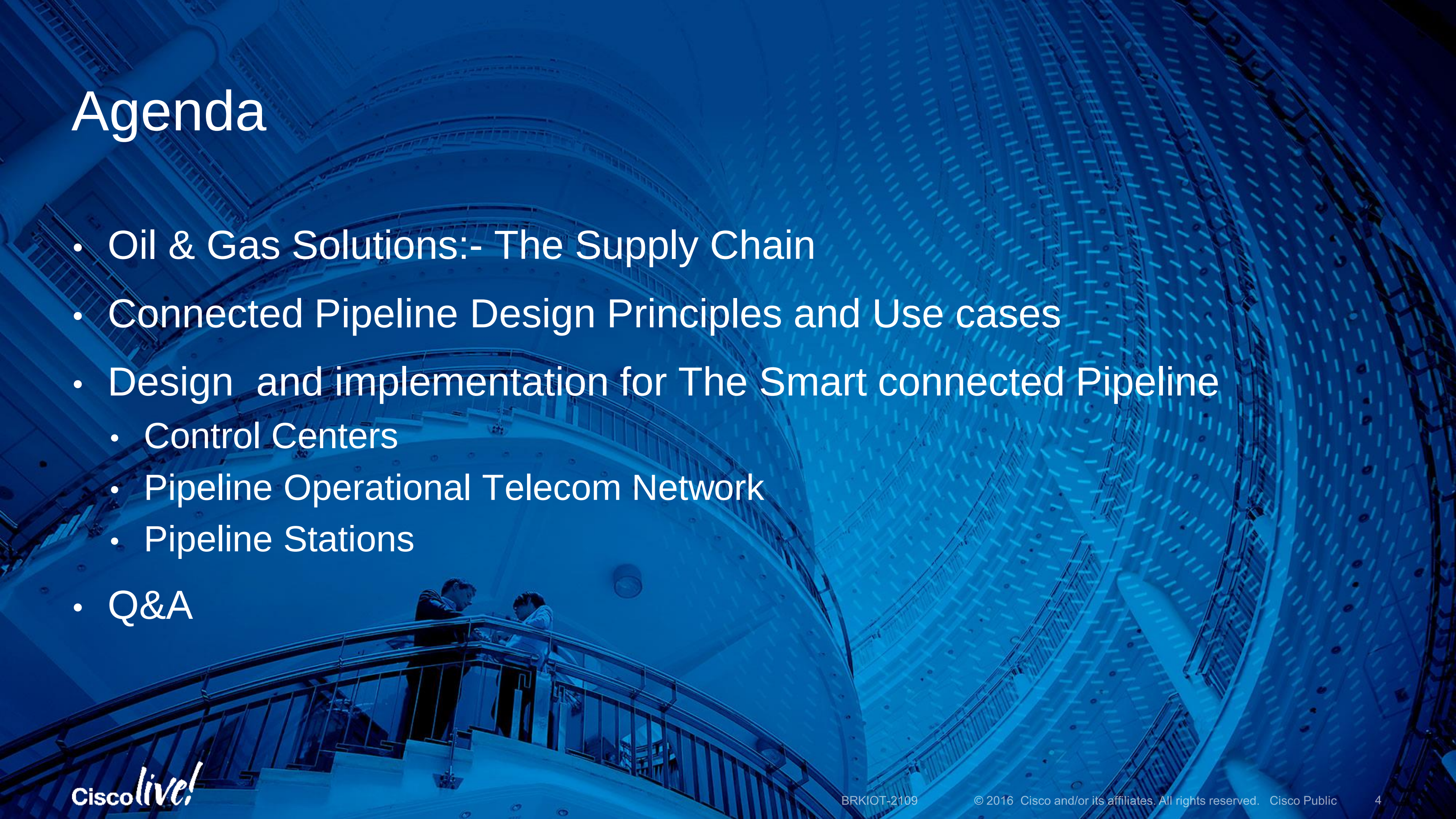
Cisco live!

Abstract

Oil & gas pipeline management is challenging. Pipelines can run over large geographical distances and through harsh environments. But it is essential that they operate as safely and efficiently as possible. Should an issue arise operators must have the capability to rapidly restore operation to meet environmental, safety, and quality requirements. How can a network be designed to support these capabilities while withstanding the same harsh conditions?

To address these unique challenges the Cisco Connected Pipeline solution delivers a unified architecture to support real time pipeline operations as well as video and collaboration services for safety and security. This session will provide an overview of the Oil and Gas supply chain, Smart Connected Pipeline SCADA design principles and then provide the design and implementation details for the Smart Connected Pipeline solution. Different options for the Virtualized Control Center design, and the connectivity options to the pipeline stations will be analyzed (including DWDM, Ethernet, and MPLS/IP). Other topics will include data center design, security, service separation, and remote access

© 2016 Cisco and/or its affiliates. All rights reserved.   Cisco Public



Agenda

- Oil & Gas Solutions:- The Supply Chain
- Connected Pipeline Design Principles and Use cases
- Design and implementation for The Smart connected Pipeline
  - Control Centers
  - Pipeline Operational Telecom Network
  - Pipeline Stations
- Q&A

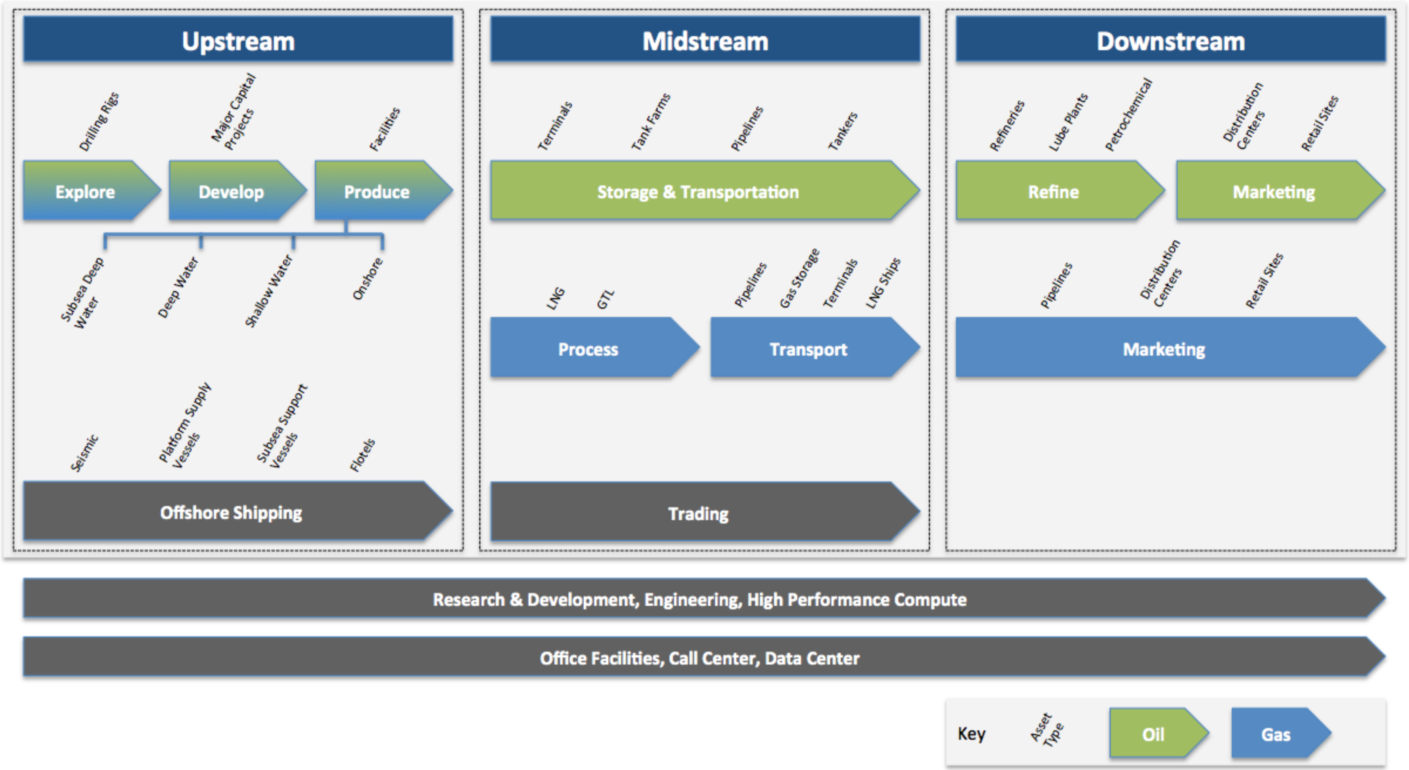
© 2016 Cisco and/or its affiliates. All rights reserved.   Cisco Public

Connected Pipelines - Overview

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

Oil & Gas Solutions:- The Supply Chain

Oil and Gas Value Chain



Upstream

Drilling Rigs
Major Capital Projects
Facilities

Explore
Develop
Produce

Subsea Deep Water
Deep Water
Shallow Water
Onshore

Seismic
Platform Supply Vessels
Subsea Support Vessels
Flotels

Offshore Shipping

Midstream

Terminals
Tank Farms
Pipelines
Tankers

Storage & Transportation

LNG
GTL
Pipelines
Gas Storage
Terminals
LNG Ships

Process
Transport

Trading

Downstream

Refineries
Lube Plants
Petrochemical
Distribution Centers
Retail Sites

Refine
Marketing

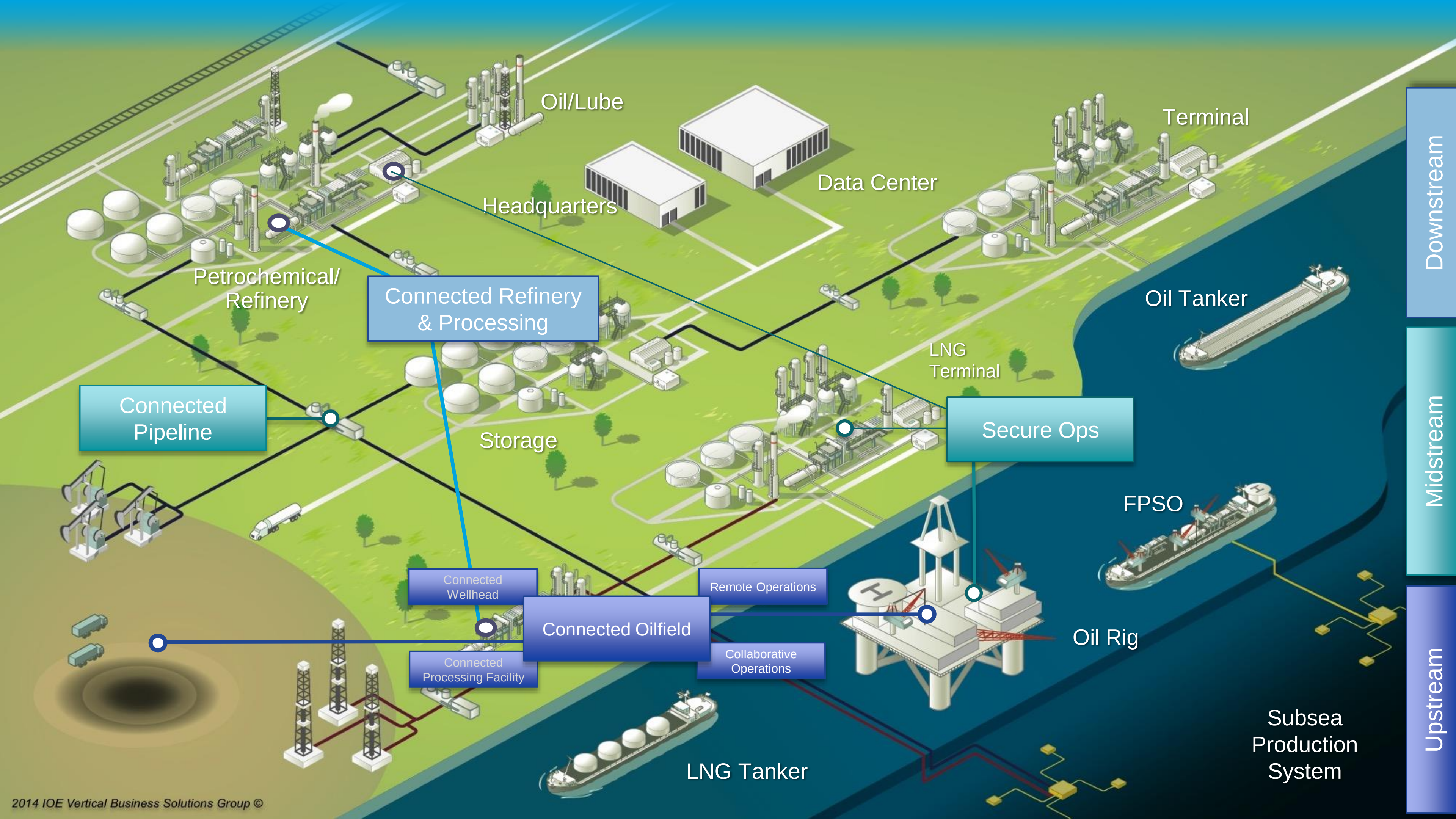
Pipelines
Distribution Centers
Retail Sites

Marketing

Research & Development, Engineering, High Performance Compute

Office Facilities, Call Center, Data Center

Key
Asset Type
Oil
Gas



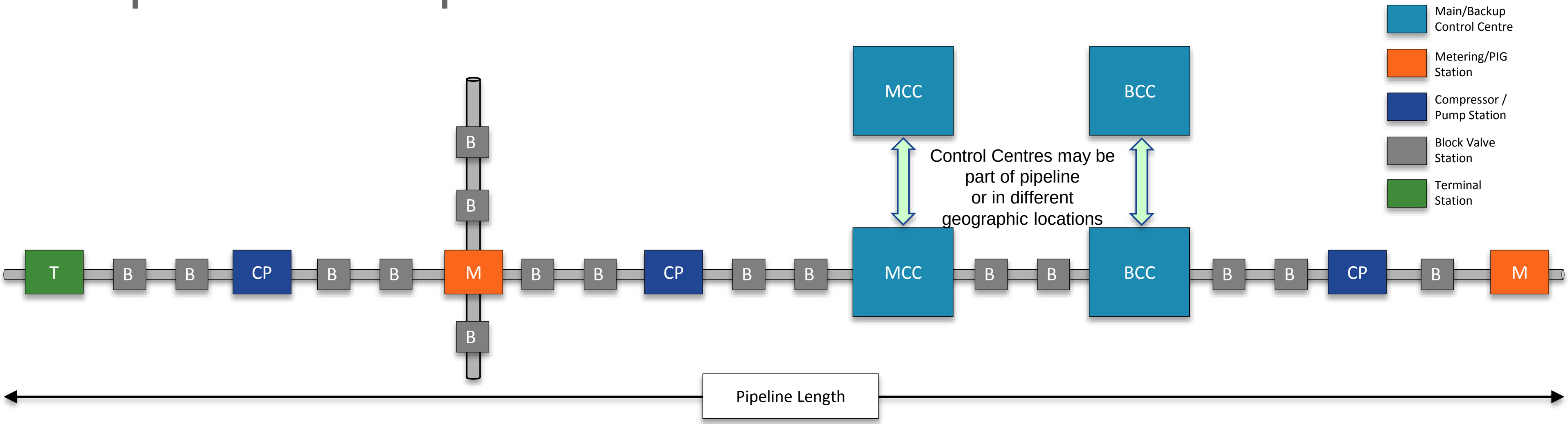
2014 IOE Vertical Business Solutions Group ©

Focus Oil & Gas Solution Overview

	Connected Pipelines	Connected Refinery	Secure Ops	Connected Oilfield
Business Outcome	**Incident Resiliency**	**Reduced Downtime**	**Secure Remote Access**	**Operational Excellence**
Key Capabilities	**Pipeline Automation** • Rapid Leak Detection • Multiservice Infrastructure • Video Surveillance • Supervisory Control • Third Party Interference Detection	**Plant Wireless** • Mobile Workforce • Remote HMI Access • Asset Tracking • People Tracking • Man Down/HSE • Industrial sensor connectivity	**Secure Ops** • Secure Remote Access • Asset Discovery/Inventory • OS Patching and AV • Situational Awareness • Identity Services	**Remote Operations** • Integrated Operations • Wellhead Monitoring • Remote Asset Monitoring • Graphics Acceleration • Distributed Analytics
Solution Highlights	• Virtualized Control Centre • Industrial security • Operational Telecoms – DWDM, MPLS, L2 Ethernet • Pipeline Station Infrastructure – Wired WAN, voice, firewall • Blueprint design - HLD/LLD	• Industrial wireless • IPICS Emergency Response • Industrial switches • Wireless Site Survey • Intrinsically safe endpoints/devices	• Secure Site and Center • ASA5500/SourceFire • 819H/CGR, Remote Mgt Svc	• ISRG2/ASR/UCS220 • Physical Security, WebEx • Remote Mgmt. Services

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

Pipeline Components Overview

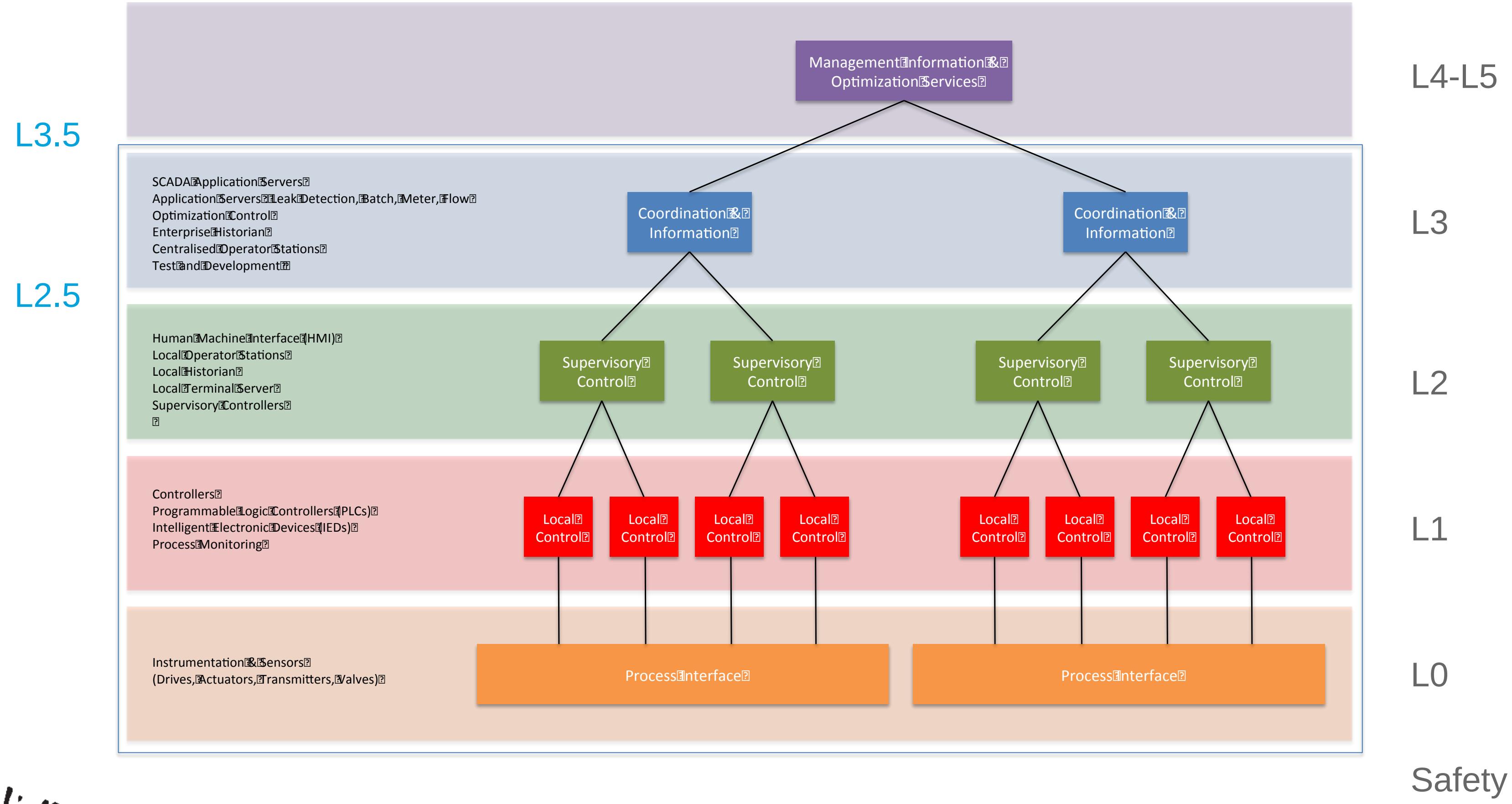


Control Centres may be part of pipeline or in different geographic locations

Component	Function
Control Centre	Monitoring and control of the pipeline system
Compressor station	Provides pressure for gas pipelines to keep flow moving
Pump station	Provides pressure for oil pipelines to keep flow moving
Metering station	Simultaneous, continuous analysis of quality and quantity being transferred in a pipeline
PIG station	Cleaning and inspecting the pipeline and flowlines
Terminal station	Where product will be delivered to end customer
Block valve station	Isolate a segment of the line for leaks or maintenance

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

Typical Pipeline Management System ISA95/99



L4-L5

Management Information & Optimization Services

L3.5

L3

SCADA Application Servers
Application Servers: Leak Detection, Batch, Meter, Flow
Optimization Control
Enterprise Historian
Centralised Operator Stations
Test and Development

Coordination & Information

Coordination & Information

L2.5

L2

Human Machine Interface (HMI)
Local Operator Stations
Local Historian
Local Terminal Server
Supervisory Controllers

Supervisory Control

Supervisory Control

Supervisory Control

Supervisory Control

L1

Controllers
Programmable Logic Controllers (PLCs)
Intelligent Electronic Devices (IEDs)
Process Monitoring

Local Control

Local Control

Local Control

Local Control

Local Control

Local Control

Local Control

Local Control

L0

Instrumentation & Sensors
(Drives, Actuators, Transmitters, Valves)

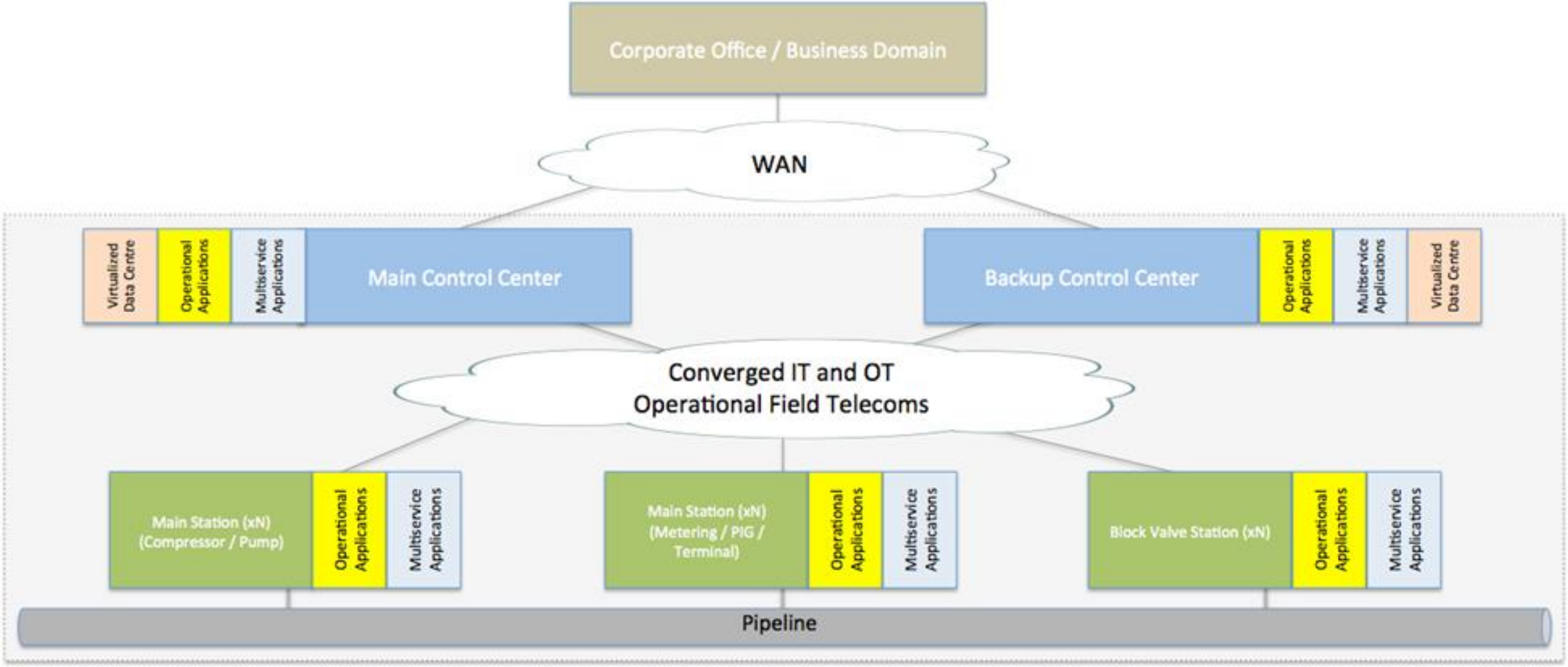
Process Interface

Process Interface

Safety

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

High Level Pipeline Architecture


Corporate Office / Business Domain
WAN
Virtualized Data Centre
Operational Applications
Multiservice Applications
Main Control Center
Backup Control Center
Operational Applications
Multiservice Applications
Virtualized Data Centre
Converged IT and OT Operational Field Telecoms
Main Station (xN) (Compressor / Pump)
Operational Applications
Multiservice Applications
Main Station (xN) (Metering / PIG / Terminal)
Operational Applications
Multiservice Applications
Block Valve Station (xN)
Operational Applications
Multiservice Applications
Pipeline

Pipeline Operating Principles

Continuous Operation: 24/7 365 days

Continuous Visibility and Control: From Control Centers to the station equipment

Safety and Compliance: Pipeline integrity, safety, security, and reliability

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

Connected Pipeline Design Principles and Use cases

SCADA Real Time Operations

- Poll, collect, store and display information from station sensors, instruments and controllers
- Send real-time control commands to stations in a reliable and fail-safe manner
- Leak detection, batch, meter and flow

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

Energy Management

- Ensuring power quality and reliable distribution
- Energy optimization
- Real time propagation and control of electrical events within the station

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

Remote Access and Decision Support

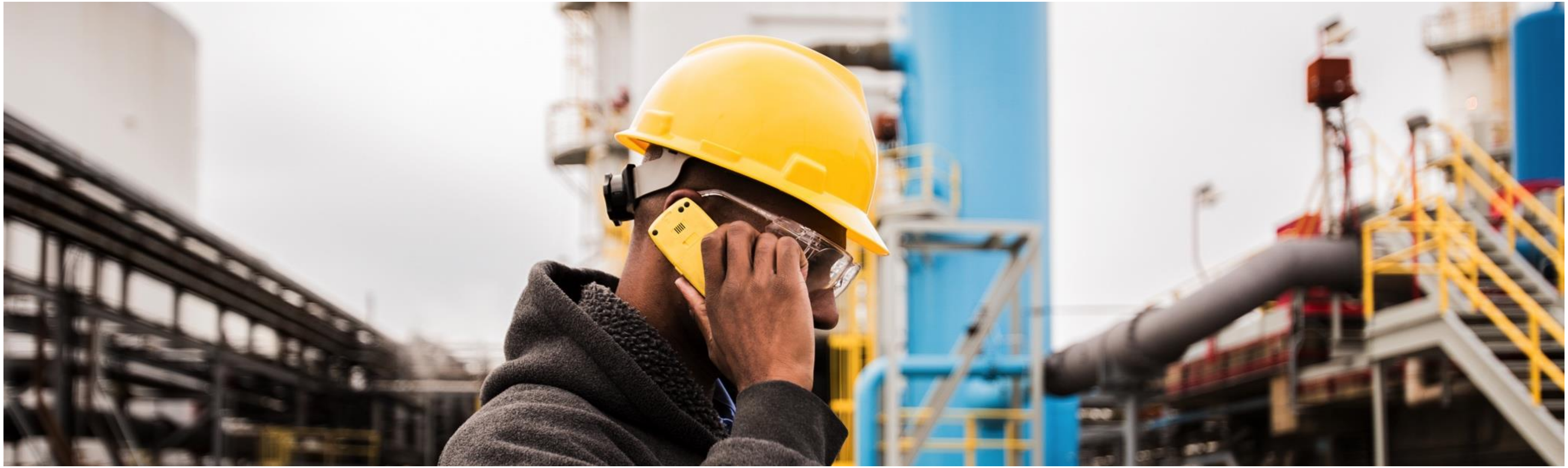
- Decision Support (DSS) Accessible Information (Level 3.5 DMZ)
- Access operational servers and content from the office, remote engineers and 3rd parties
- Remote access to the Process control domain (Levels 0-3 of the Purdue model)
- Access office (Levels 4-5 of the Purdue model) resources from the process domain.

Advanced Leak Detection / Intrusion Detection

- Distributed Acoustic Sensing
- TPI (Third party intrusion)
- Environmental monitoring

Physical Security

- Pipeline station internal and external CCTV
- Access Control Systems
- High Quality Video stream to Control Center from pipeline stations



Voice and Emergency Response

- Broadcast emergency announcements to remote stations
- Integrate IP / landline voice, mobile, radio, video, and emergency response services

Mobile Worker

- Pipeline station mobility services
- Integrated workflow
- Pipeline inspection

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

Asset Health and Predictive Maintenance

- Asset monitoring
- Preventive, predictive, and prescriptive maintenance
- Supply chain integration

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

Pipeline Architecture Design Principles

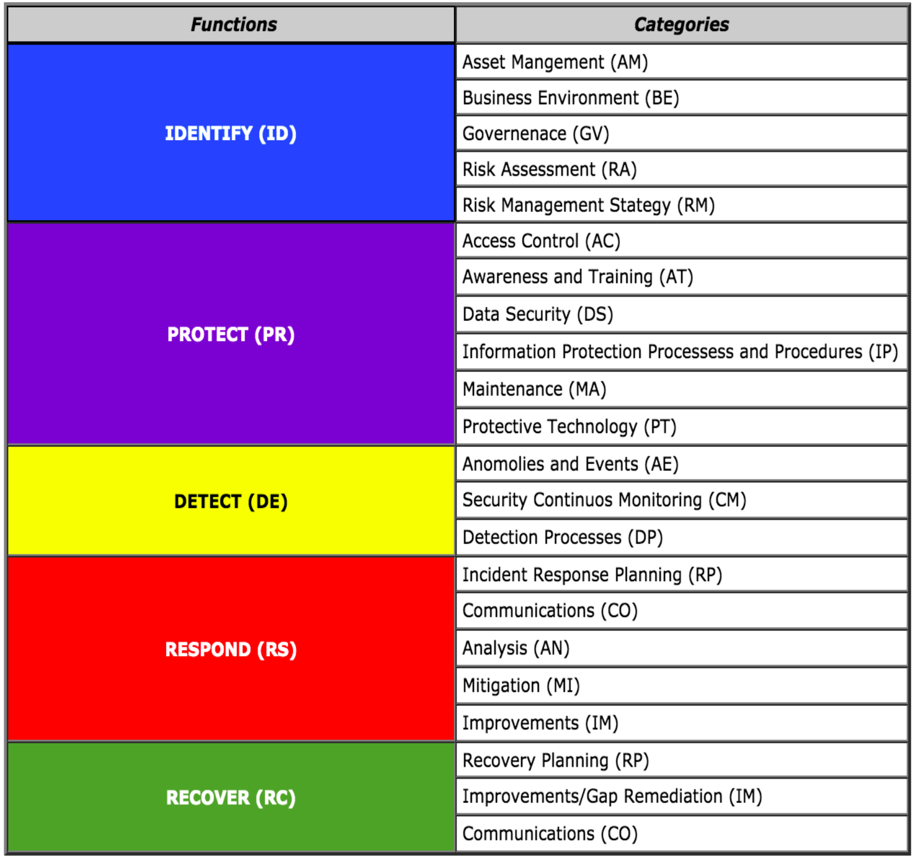
The pipeline operator must have **control of the pipeline 24/7/365 and maintain control of the pipeline** …akin to an Air traffic Controller

- **High Availability :** redundancy and reliability mechanisms at all levels
- **Multi-Level Security :** physical and cyber attacks, and non-intentional security threats
- **Multiservice Support :** operational and non-operational applications coexisting on a communications network
- **Integrated Management :** network, security, and administration management, from the instrumentation or sensor to the control-center application and operators
- **Open Standards :** based on IP with transport of traditional serial protocols, interoperability between current and future applications

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

Key Standards for Oil & Gas Pipeline Security

- ISA95 / Purdue Model of Control
- ISA99 / IEC 62443
- NIST Cybersecurity Framework
- ISO 27001
- NERC-CIP*
- Industry specific
  - *For Example; American Petroleum Institute API Standard 1164* for SCADA security



Functions	Categories
IDENTIFY (ID)	Asset Mangement (AM)
	Business Environment (BE)
	Governenace (GV)
	Risk Assessment (RA)
	Risk Management Stategy (RM)
PROTECT (PR)	Access Control (AC)
	Awareness and Training (AT)
	Data Security (DS)
	Information Protection Processess and Procedures (IP)
	Maintenance (MA)
	Protective Technology (PT)
DETECT (DE)	Anomolies and Events (AE)
	Security Continuos Monitoring (CM)
	Detection Processes (DP)
RESPOND (RS)	Incident Response Planning (RP)
	Communications (CO)
	Analysis (AN)
	Mitigation (MI)
	Improvements (IM)
RECOVER (RC)	Recovery Planning (RP)
	Improvements/Gap Remediation (IM)
	Communications (CO)

** North America Power Utilities – but emphasises physical perimeters*

© 2016 Cisco and/or its affiliates. All rights reserved.   Cisco Public

Pipeline Design Principles - Security

IEC 62443 – Key Fundamental Security Requirements

- **Identification, Authentication & Control (IAC) (ISA-62443-3-3 FR 1):** Identify and authenticate all users (humans, software processes and devices)

- **Use Control (UC) (ISA-62443-3-3 FR 2):** Enforce user privileges to perform the requested action and monitor use

- **Data Confidentiality (DC) (ISA-62443-3-3 FR 4)**: Confidentiality of information on communication channels and in data repositories

- **Restricted Data Flow (RDF) (ISA-62443-3-3 FR 5)**: Segmentation and zoning with conduits to allow data flow

- **Timely Response to Events (TRE) (ISA-62443-3-3 FR 6)**—Respond to security violations by notifying the proper authority, reporting needed evidence of the violation and taking timely corrective action when incidents are discovered

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

Pipeline Design Principles - Multiservice

- Operational and non-operational applications over a **shared networking infrastructure**

- **Logical or physical segmentation** isolation between critical and non critical systems and services to protect against cross pollination of traffic/services

- **Prioritization of services** over shared infrastructures …… operational traffic trumps all

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

Pipeline Design Principles - Management

- Network and security infrastructure is a **core component of the PLMS**
- **Operator needs visibility** into infrastructure and security performance
- **Correlation** of infrastructure and security alarms and alerts with PLMS alarms and alerts

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

Pipeline Design Principles – Open Standards

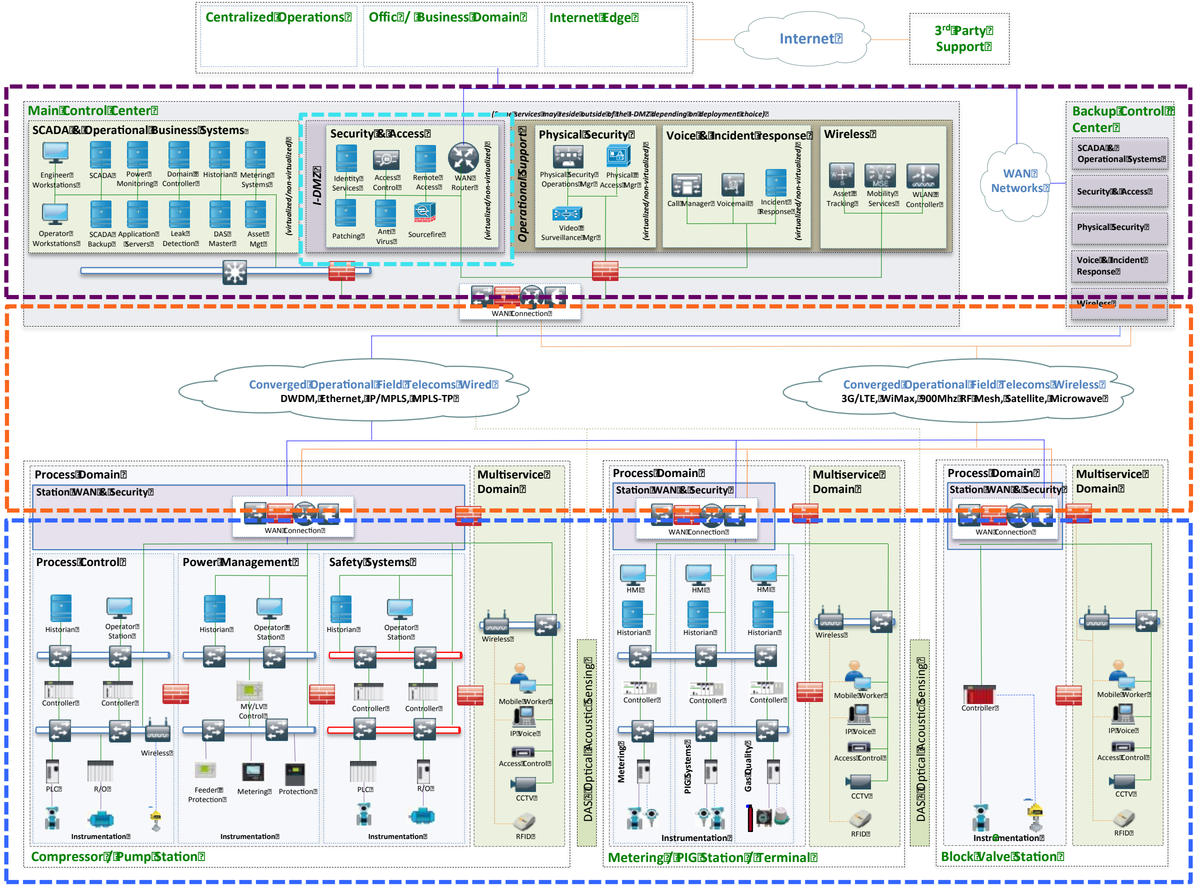
- **Multi-vendor Environment**: Architecture is vendor agnostic and creates joint system solutions
- **Maintainability:** Promotes industry standards for future-proofing, interoperability and reduced silos
- **Cost Efficiency:** Allows infrastructure convergence and consolidation of resources (dependent on customer philosophy) helping (TCO) for the Pipeline System
- **Versatility:** New use cases and functionality to increase system availability, security, safety, and system performance

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

Connected Pipelines Reference Architecture

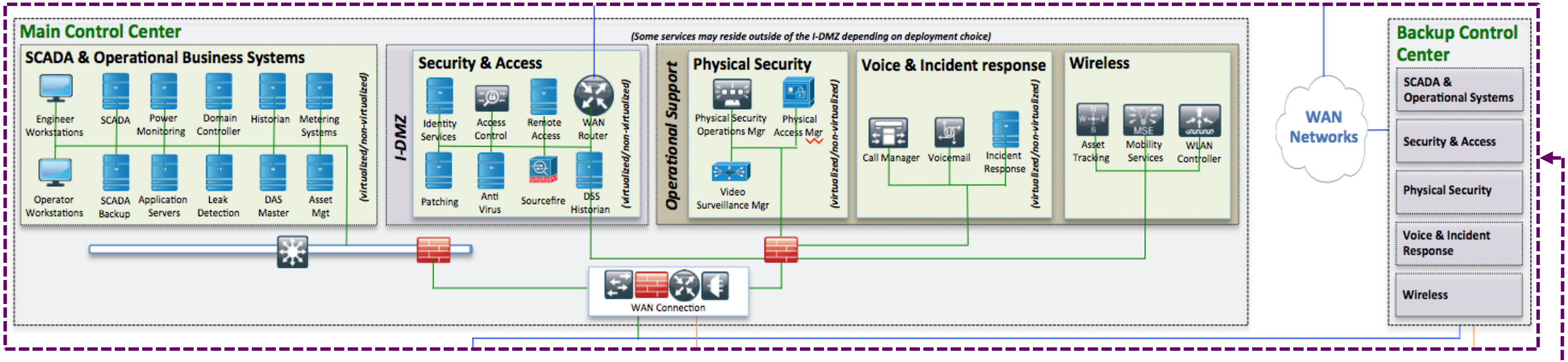
Forward-looking functional architecture for end-to-end pipeline infrastructure:

- A flexible, modular approach that supports a phased **Oil and Gas Pipeline** operational excellence
- End to End Integrated Solution for Process , Safety , Power & Security
- Control Room Virtualization
- Converged Wide Area Operational Telecoms
- Pipeline Station Wired and Wireless Networks
- Integrated Multi-Service use cases
- IEC 62443 / ISA99 Security model



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

Connected Pipelines Control Centre Overview



Virtualized Control Centre

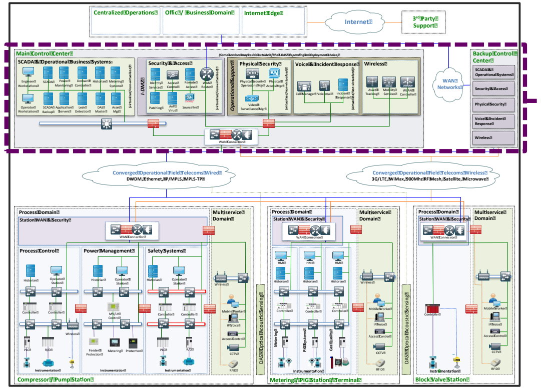
- Virtualized pipeline management system applications
- Centralized multiservice and physical security functions

SCADA & Operational Systems

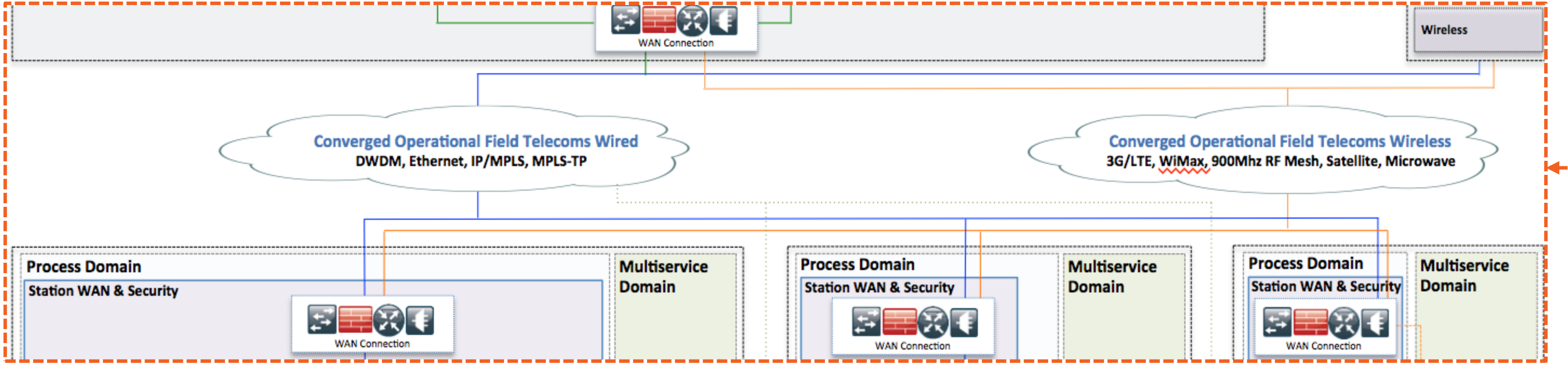
- UCS, Nexus, SAN

Multiservice

- UCS, Appliance, DC Switching
- Operations Manager, Access Manager, Video Surveillance Manager
- CallManager, Voicemail
- WLC, MSE



Connected Pipelines Operational Telecoms Overview



Operational Field Telecoms

- Connectivity between pipeline stations, stations to Control Centers, Control Center to Control Centre.
- Security at Level 2.5 for station protection

Wired

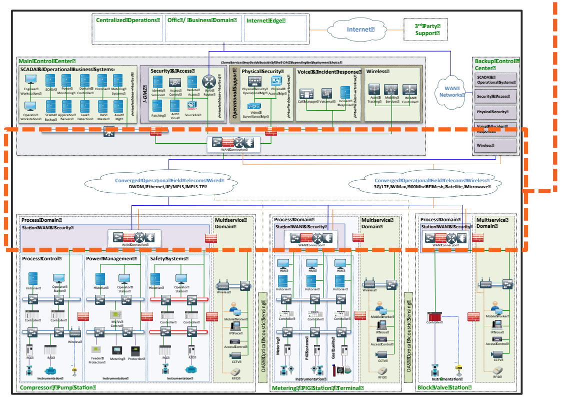
- DWDM, Ethernet, IP/MPLS, MPLS-TP
- ONS, ASR90X, IE2K/3K/4K

Wireless

- 3G/LTE, Satellite, WiMax, Microwave
- 819H, 829, 809

Security

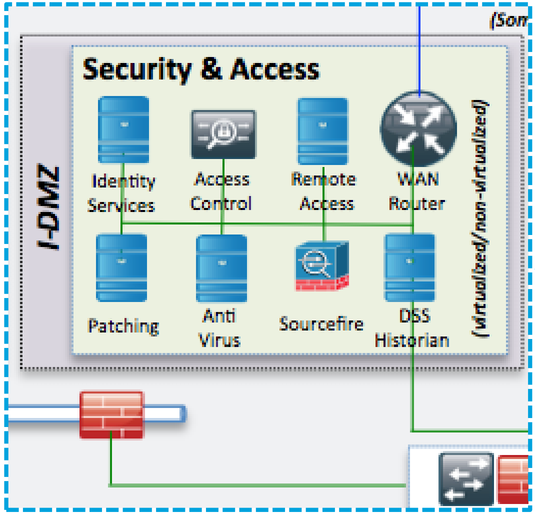
- ISA3000, ASA55XX

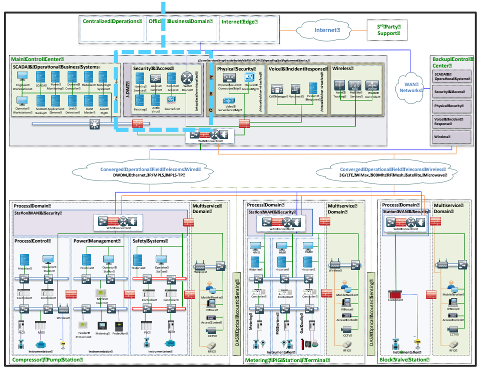


Cisco live!

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

Connected Pipelines Security and Support Overview





Security Services and Secure Remote Access

- Delineation between business and operational domains
- Secure remote access into operational domain
- Non-real time operational data access
- Centralised security functions

I-DMZ (L3.5)

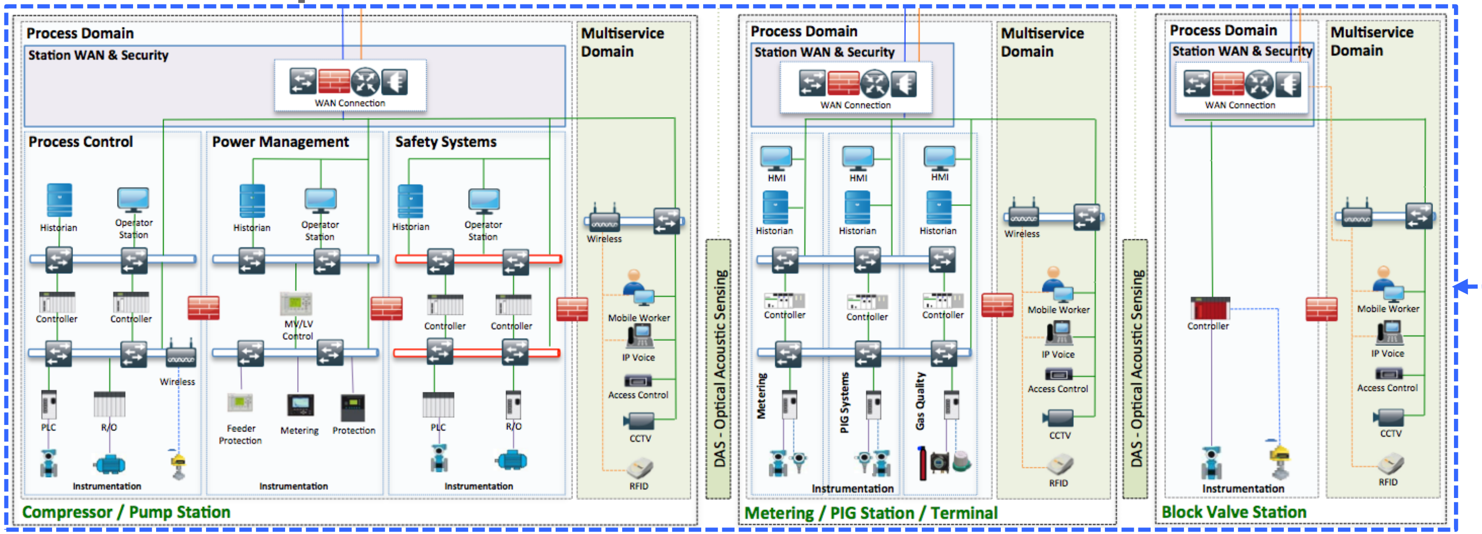
- UCS, ASA, Patching updates, Anti Virus
- Jump Server, VPN remote access

Security

- ISE (Identity Services Engine), Sourcefire, NAC (Network Access Control), SIEM

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

Connected Pipelines Station Overview



Pipeline Stations

- Operational - Process control, power management, safety systems, PIG, metering
- Multiservice – Mobile worker, voice, physical security

Industrial wired networks

- IE2K/IE3K/IE4K, CGS

Industrial wireless networks

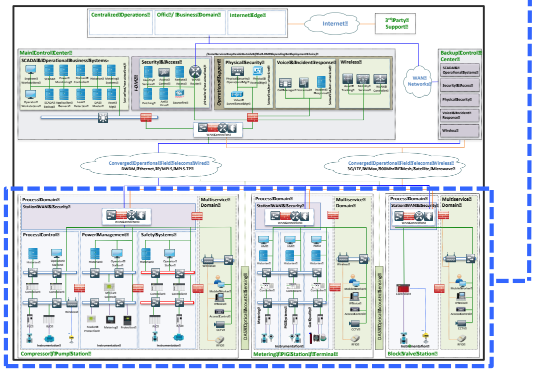
- 1552H/S/WU, IW3702

Industrial security

- ISA3000

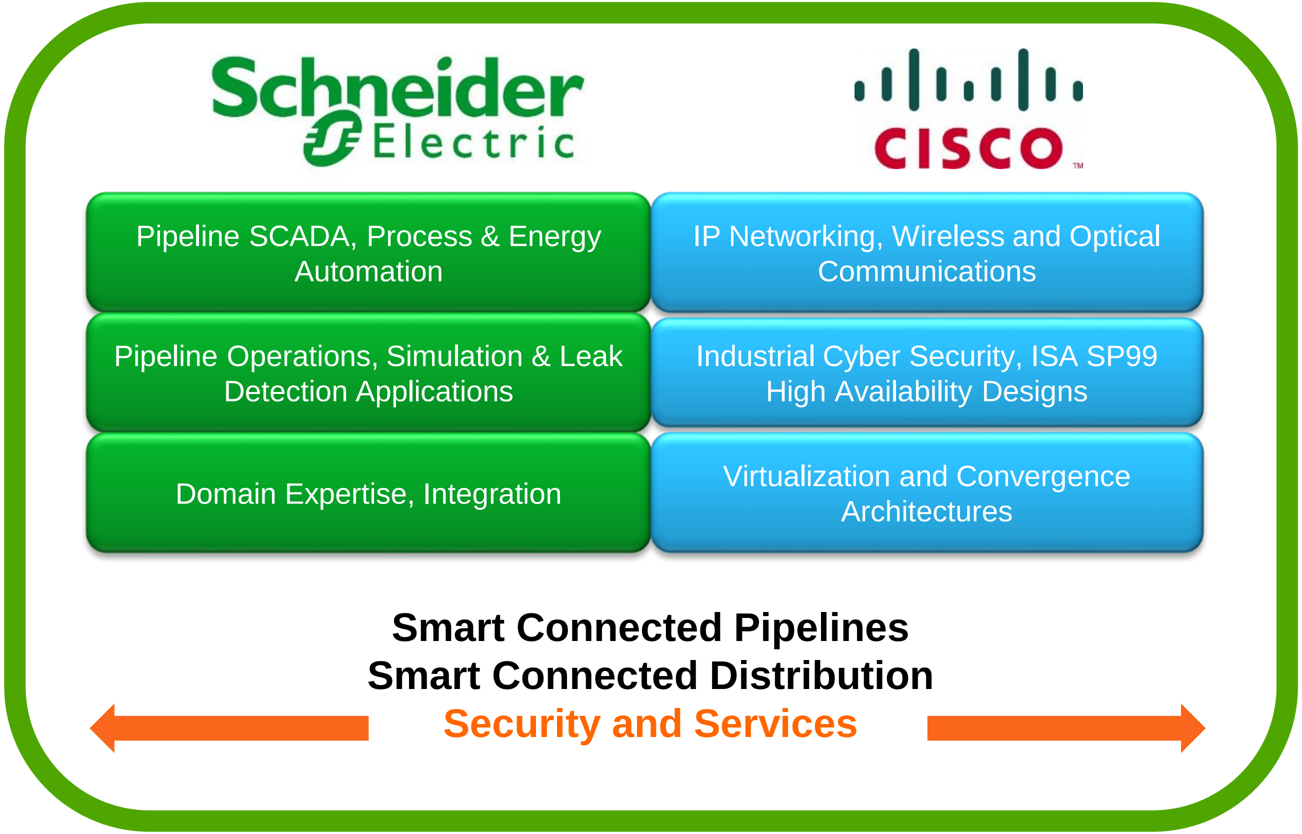
Station edge and security

- ISA3000, ASA55XX



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

Partnership Approach



Schneider Electric

Cisco

Schneider Electric	Cisco
Pipeline SCADA, Process & Energy Automation	IP Networking, Wireless and Optical Communications
Pipeline Operations, Simulation & Leak Detection Applications	Industrial Cyber Security, ISA SP99 High Availability Designs
Domain Expertise, Integration	Virtualization and Convergence Architectures

Smart Connected Pipelines
Smart Connected Distribution
Security and Services

Key Pipeline Partners

Schneider Electric
Rockwell Automation
ABB
Honeywell

Cisco Validated Design (CVD) program – **“Smart Connected Pipeline”**

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

Connected Pipelines – Design and Implementation

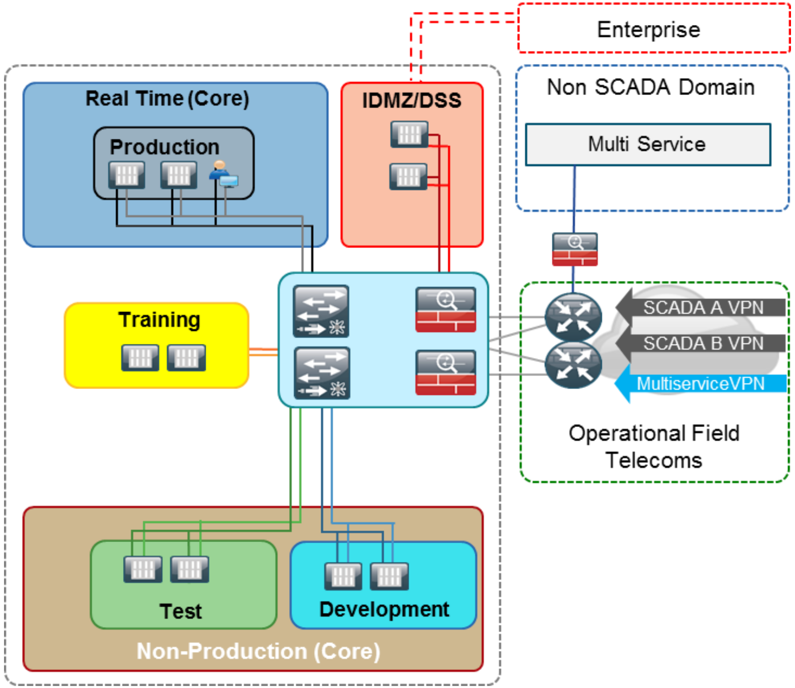
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

Design & Implementation

Control Centers

Control Center Environments

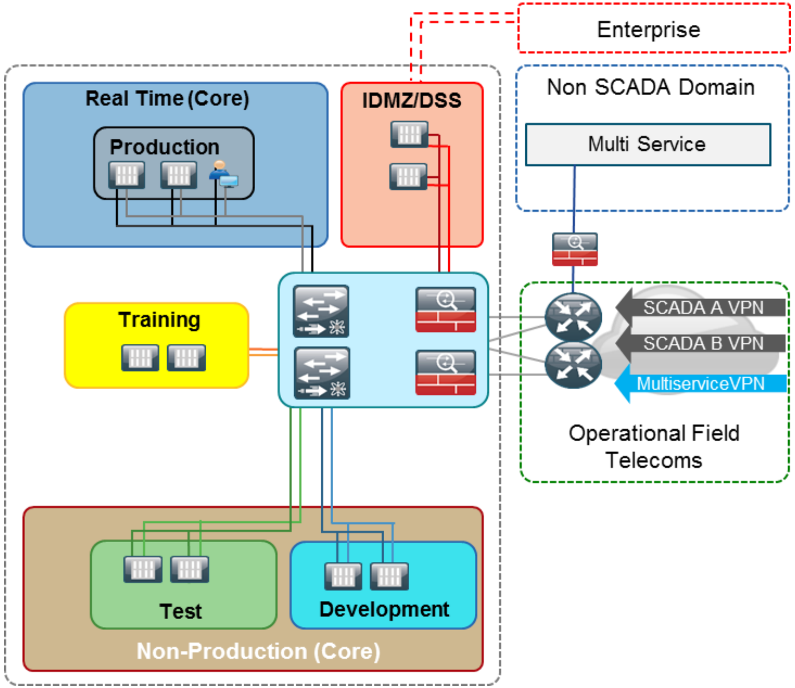
- Production Environment
- Test
- Development
- Training
- Decision Support System (DSS)



FOR YOUR REFERENCE

Production Environment –Real Time Operations

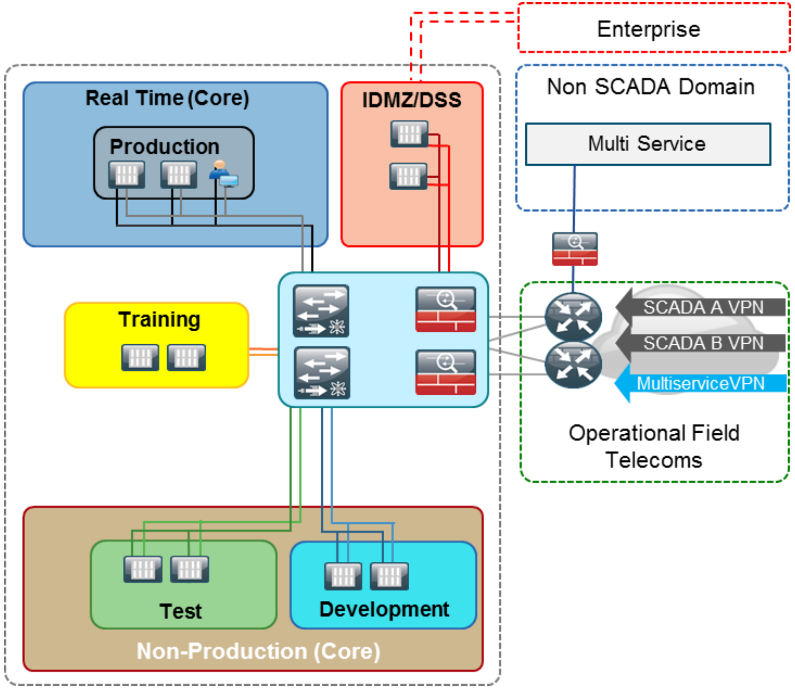
- Real Time Servers
  - Provides monitoring and control for the SCADA system
- Domain Controller
  - Dedicated for SCADA
- Logging Server
  - OASyS Logs, Data playback, windows events
- Deployment Server
  - Display & database commissioning
- Historical Servers
  - Long term storage of Real-Time measurement, event, alarming & data generated by the SCADA system
- Leak Detection Server
- Operator Work stations



FOR YOUR REFERENCE

Test & Development

- Test System
  - Non production replica of the operational SCADA system
  - Code/config change validation prior to production implementation
- Development System
  - Code and Database maintenance
  - Store and edit Baseline/Custom displays
  - Initial platform for configuration of additional machines in the domain

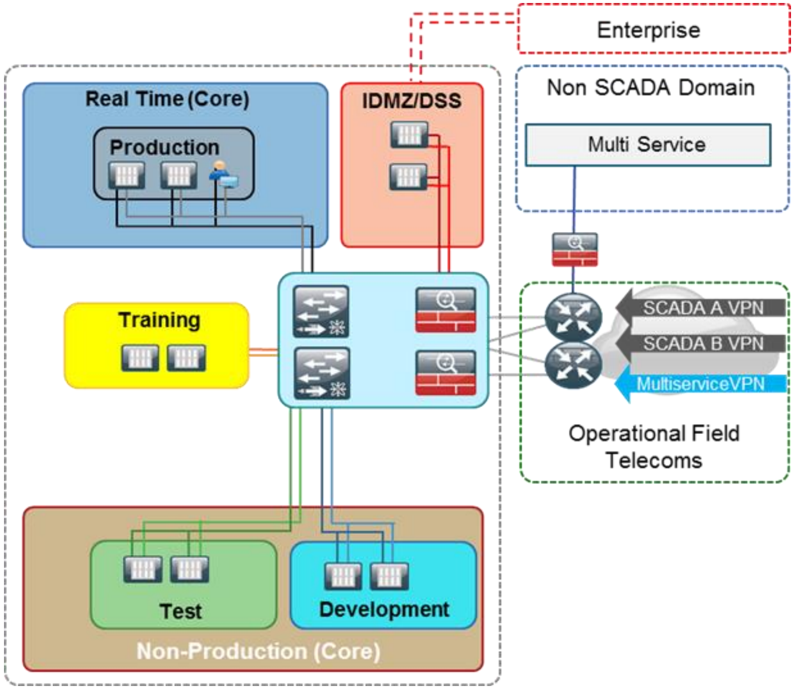


© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

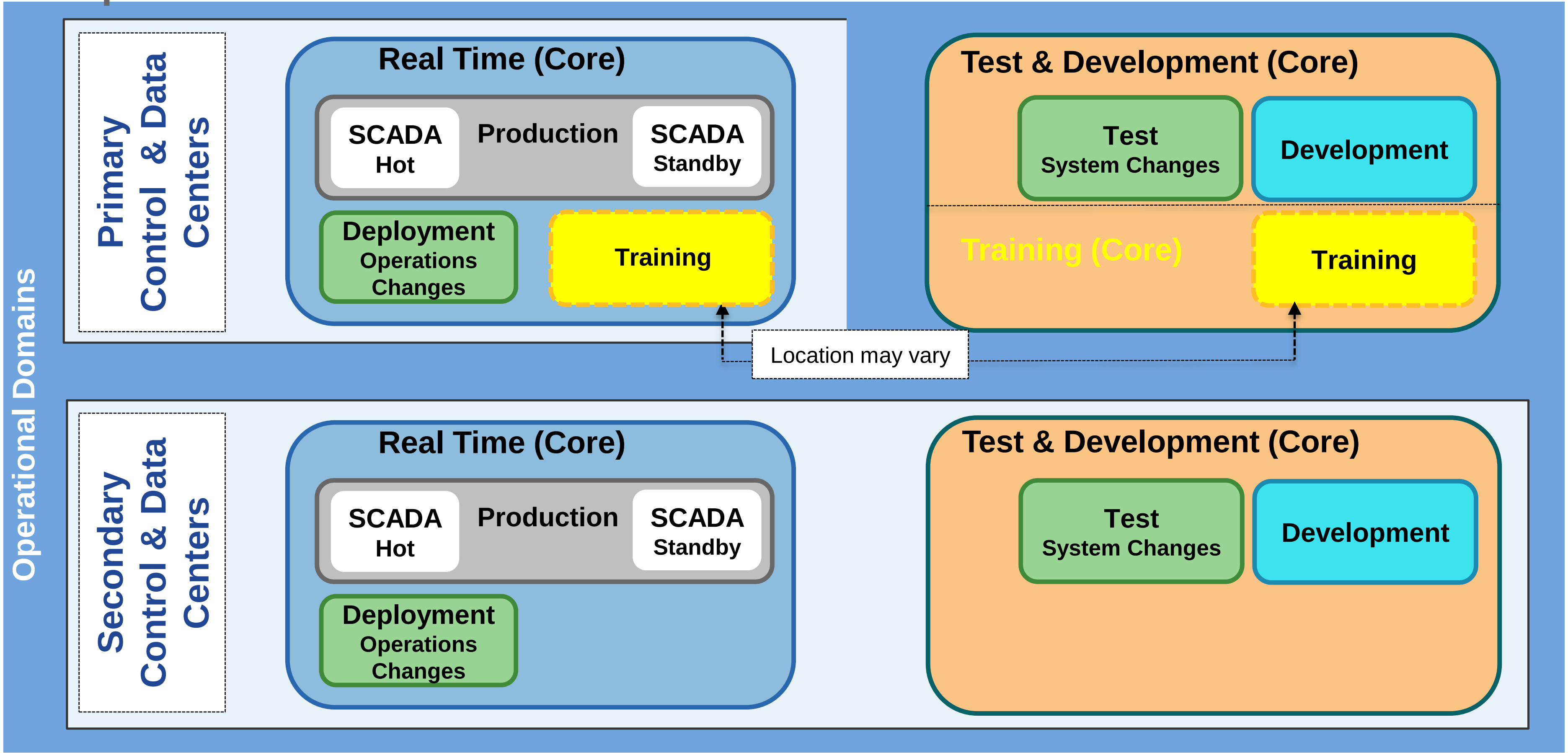
FOR YOUR REFERENCE

Decision Support System

- Industrial DMZ Environment
- Isolates operational system from external systems or users.
- Receives Real-time and historical updates from Production
- Secure Remote Access Services
  - Remote Desktop and Remote Client Service (RCS)
- DSS Servers
  - Historical & Real Time Servers
  - DMZ Domain Controllers



Operational Domains Overview



Operational Domains

Primary Control & Data Centers

Real Time (Core)

SCADA Hot

Production

SCADA Standby

Deployment Operations Changes

Training

Test & Development (Core)

Test System Changes

Development

Training (Core)

Training

Location may vary

Secondary Control & Data Centers

Real Time (Core)

SCADA Hot

Production

SCADA Standby

Deployment Operations Changes

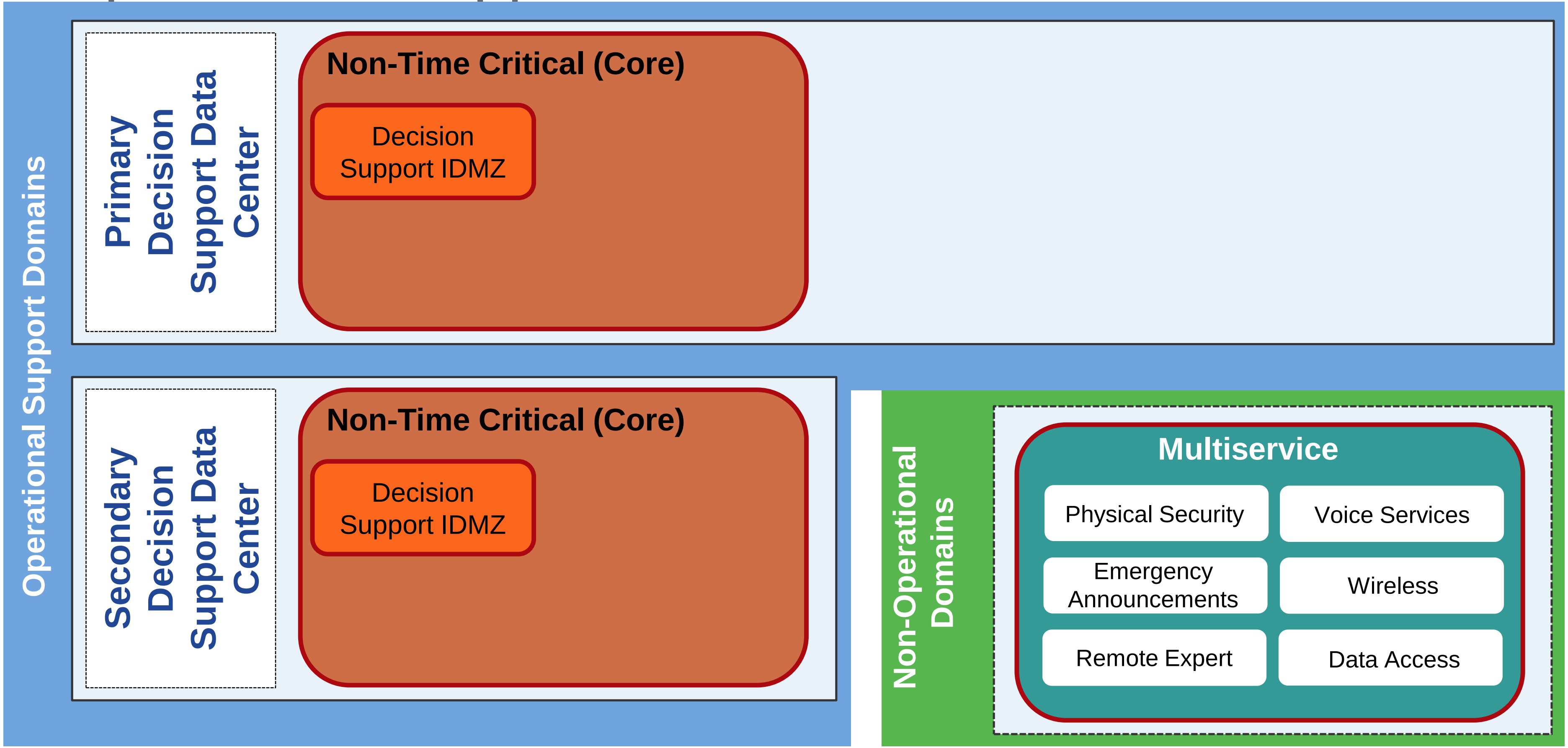
Test & Development (Core)

Test System Changes

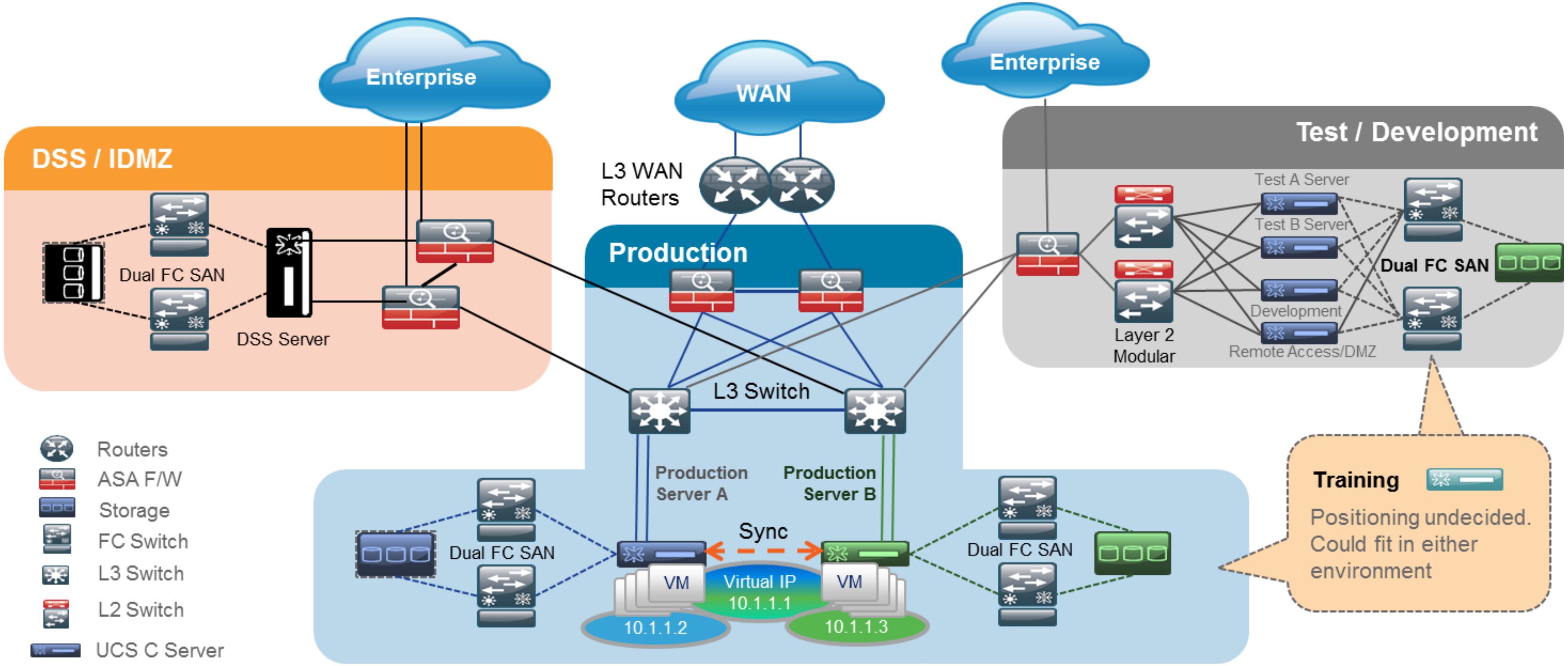
Development

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

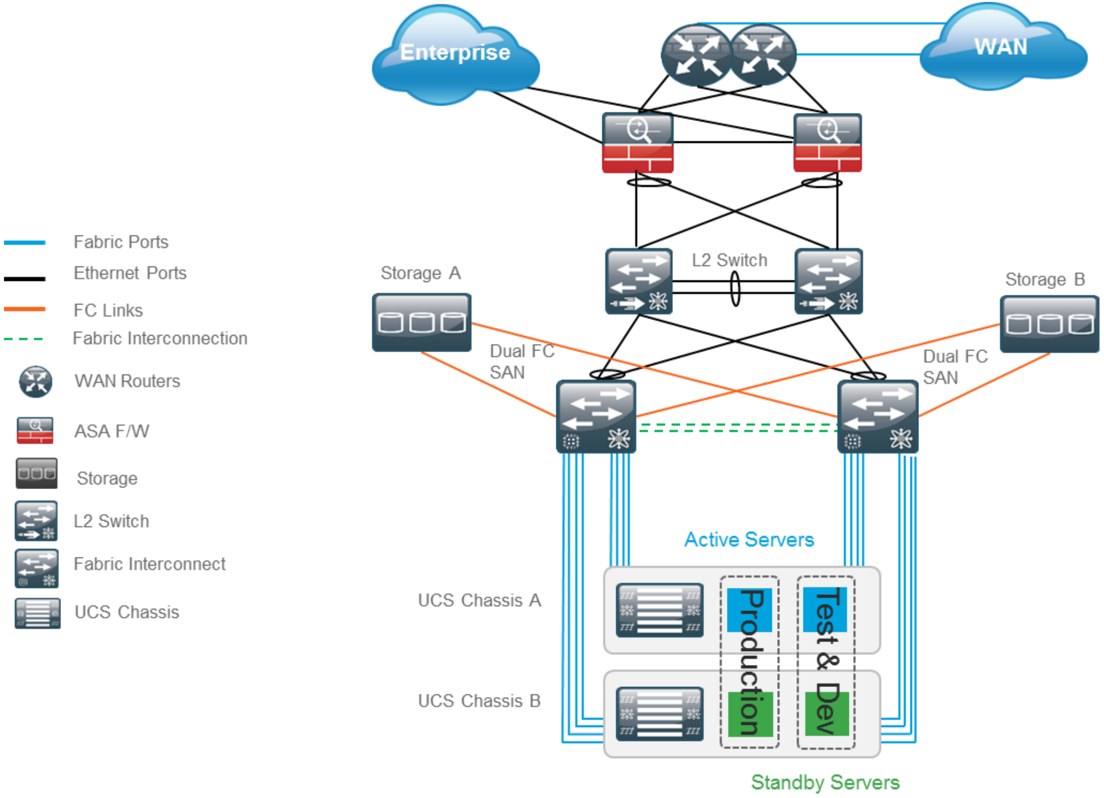
Operational Support Domains Overview



SCADA Deployment – Physical Separation



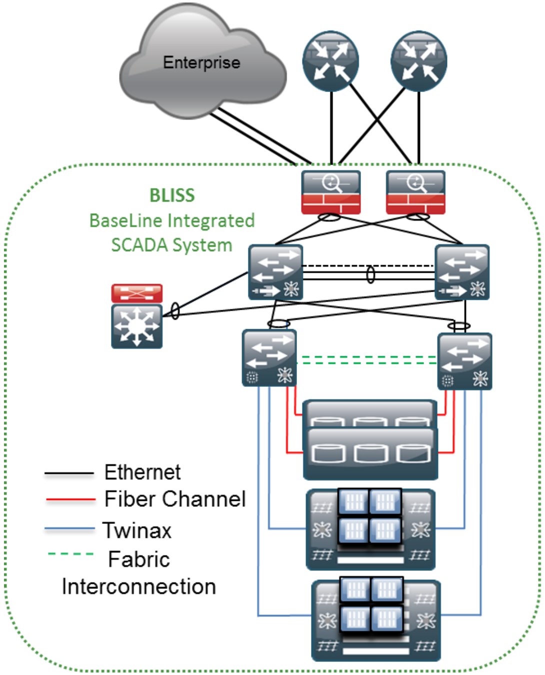
SCADA Deployment – Consolidated Architecture



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

Control Center Validated Design

BaseLine Integrated SCADA System (BLISS)



WAN Routers

Dual ASA 55X5-x
Firewalls Active/standby

Dual Nexus 3524 vPC Connectivity
with ASA, 3850 & UCS

3850 stack switching operator
workstation connectivity

Dual UCS Fabric Interconnects

2 x Direct Attached Storage arrays
to UCS Fabric Interconnects

2 x UCS Chassis with
B200 M4 servers

2x B200 M4 servers per
SCADA Zone

Network

2x ASR 902
2 x Nexus 3K
2 x Catalyst 3850

Compute

Microsoft System Center

2 x UCS 6248UP Fabric
Interconnects

2 X UCS 5108
16 x UCS B200 M4 (8 per
chassis)

Storage

2 x EMC VNX 3200
Storage Array
Directly Attached
Storage to Fabric
Interconnects

Security

2 x ASA 55x5-X

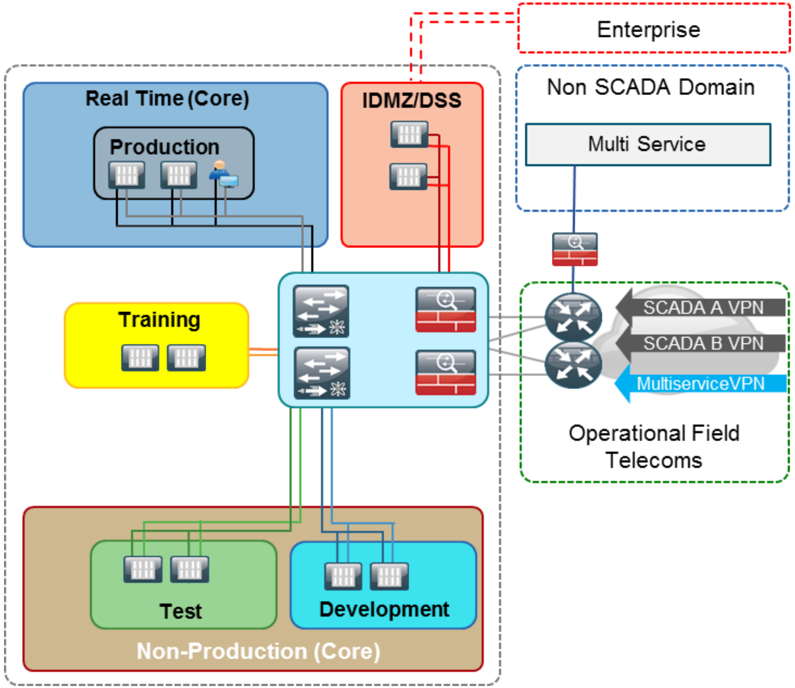
Security Overview

- Data Confidentiality and Privacy, methods such as segmentation, protecting against unauthorized access and encryption of the data.
  - *Data Confidentiality (DC) (ISA-62443-3-3 FR 4)*
- Segmentation and isolation using Zones and conduits. Isolate each of the environments into zones that share a common set of security requirements or functions.
  - *Restricted Data Flow (RDF) (ISA-62443-3-3 FR 5)*
- Restrict data flow between zones using Firewalls, Access lists, IDMZ
  - *Restricted Data Flow (RDF) (ISA-62443-3-3 FR 5)*
- Threat Detection and mitigation using the Firewalls, IDS devices
  - *Timely Response to Events (TRE) (ISA-62443-3-3 FR 6)*
- Access Control to resources to which a user or device is authorized to access. Authentication, authorization and accounting, RBAC.
  - *Identification, Authentication & Control (IAC) (ISA-62443-3-3 FR 1)*
- Industrial DMZ & DSS to isolate the operational system from any external systems or users.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

Control Centre Segmentation

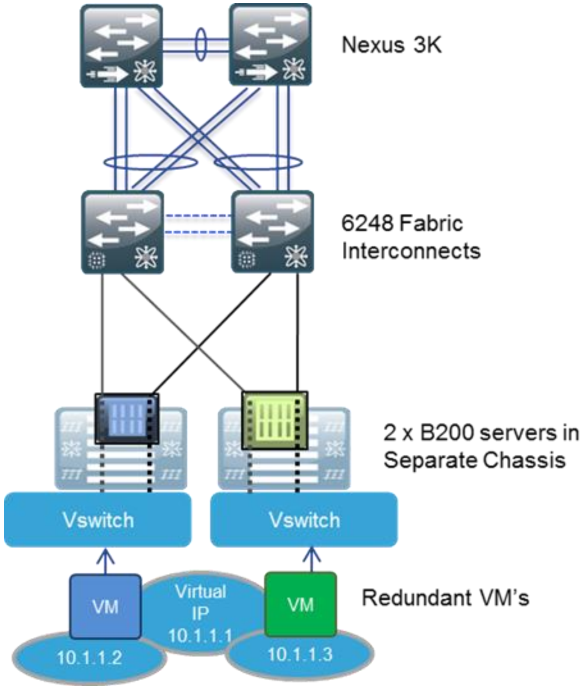
- Zones isolated by Layer 2 VLAN inside Control Centre
- L3 Gateway enabled at the ASA enforcing policy
- No inter-zone traffic without explicit configuration
- Operator Workstations in the same L2 VLAN as the SCADA services
- Traffic separation across Operational WAN, and maintained in Control Centre
- Segment Multiservice from SCADA



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

Compute Segmentation

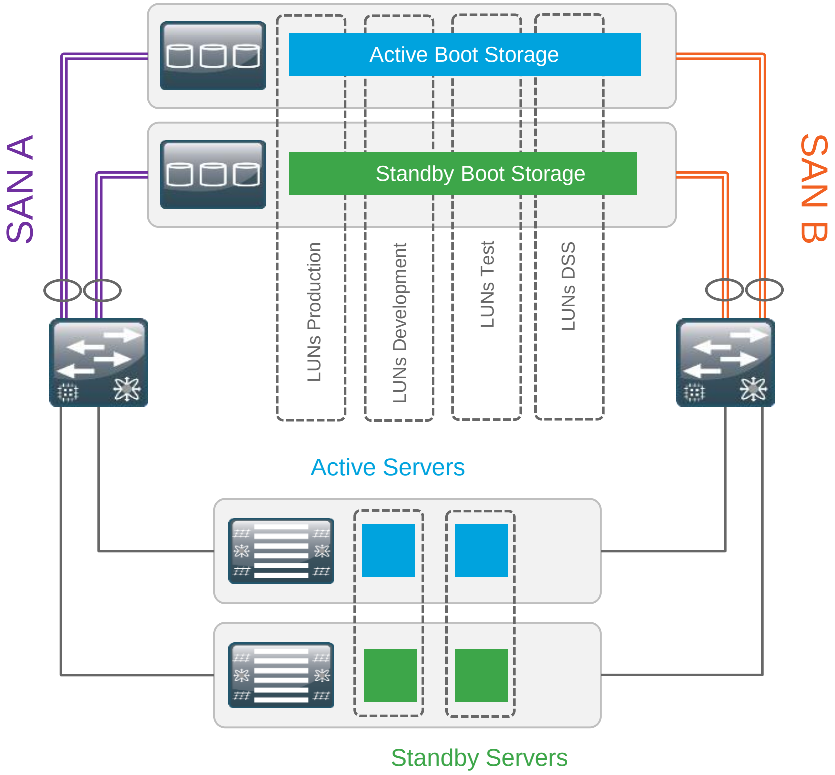
- Dedicated Physical Servers per environment
- Servers separated in two UCS Chassis Main/Alternate
- VM's are utilize a vSwitch. VLAN, QoS and security policies can be applied closer to the edge
- VLAN Segmentation from the VM through the vSwitch, UCS system, Nexus 3524 to the ASA



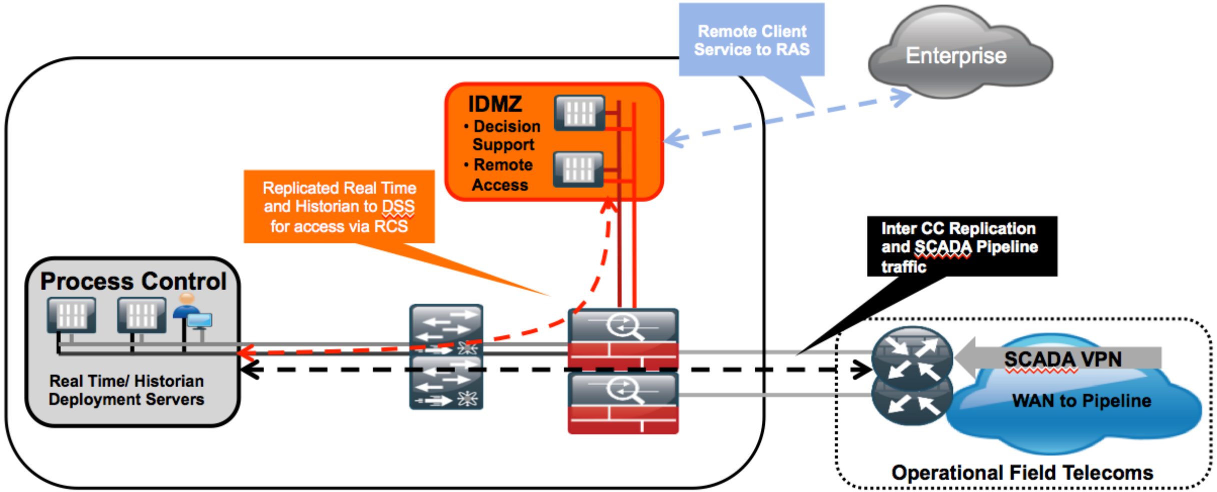
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

Storage Segmentation

- Dual Storage Arrays, each serving different hosts and physical servers on each UCS Chassis
- Segmentation using VSANS, FC Zoning and LUNs.
- FC Zoning on the UCS with direct connect allows for physical server mapping to a storage controller/array
- Logical Unit Number (LUN) restricts storage LUN access to specific hosts on the shared SAN



Firewall Architecture


Remote Client Service to RAS
Enterprise
IDMZ
• Decision Support
• Remote Access
Replicated Real Time and Historian to DSS for access via RCS
Inter CC Replication and SCADA Pipeline traffic
Process Control
Real Time/ Historian Deployment Servers
SCADA VPN
WAN to Pipeline
Operational Field Telecoms

- Security between the Control Center to the pipeline and to the Backup Control Center
- Provide Intra Control Center policy between zones and segments
- Provide an Industrial DMZ for operational data which can be accessed by the enterprise, and a secure staging area for patching and anti-virus services.

© 2016 Cisco and/or its affiliates. All rights reserved.   Cisco Public

Control Center Industrial DMZ

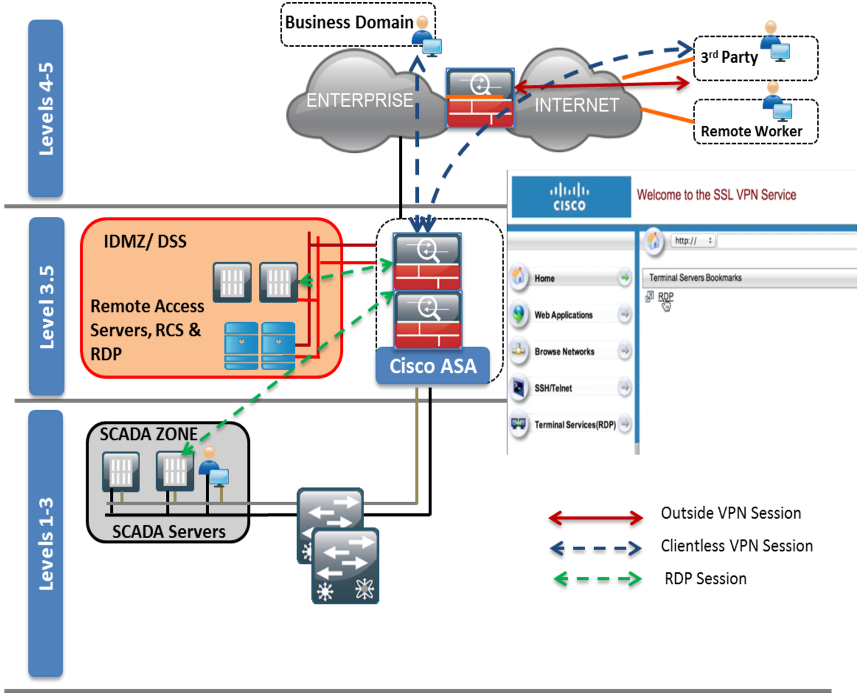
- No direct communications between the Enterprise and the PCD
- Create security policies to explicitly allow authorised communications into the PCD and prevent unauthorised communications
- Provide secure communications between the Enterprise and the PCN using “mirrored” or replicated servers and applications
- The IDMZ provides remote access services into the PCD
- Create security policies to explicitly allow authorised communications into the PCD and prevent unauthorised communications

“Alignment with IEC 62443/ISA99 and ISA 95 requirement in the Process control domain (PCD) to provide strict policy enforcement between the trusted levels 1-3 of the PCD and the untrusted levels 4-5 of the Enterprise/business domain”

© 2016 Cisco and/or its affiliates. All rights reserved.   Cisco Public

Secure Remote Access

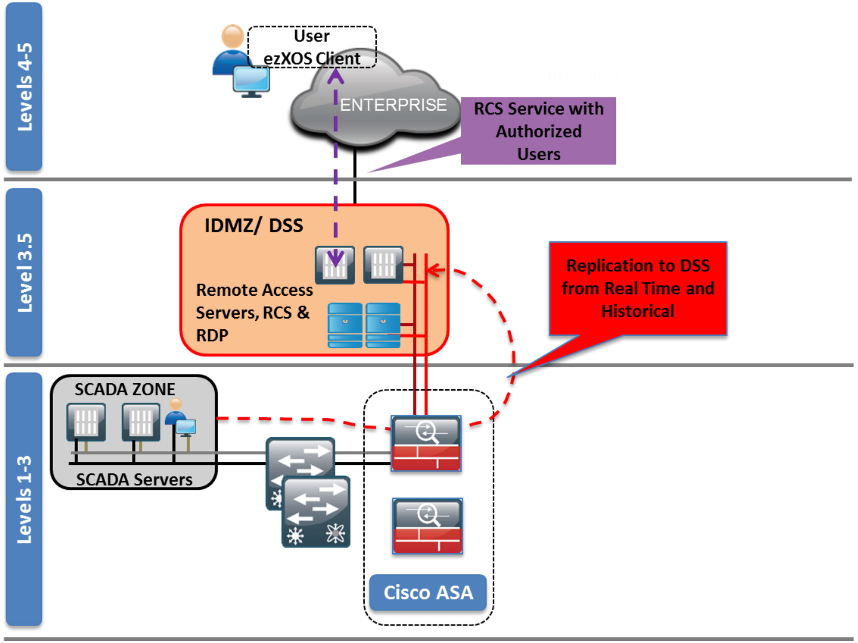
- RDP sessions via the SSL VPN portal
- User uses Clientless VPN service to the ASA using a web browser and its SSL encryption
- User is authenticated against AD and presented with a bookmark or bookmarks based on their policy
- User is restricted form any direct access on the network



© 2016 Cisco and/or its affiliates. All rights reserved.   Cisco Public

RCS Remote Client Service

- OASyS DNA RCS provides remote access to SCADA applications without the client being a member of the control system domain
- The client communicates with the RCS server in the DMZ
- The RCS server queries data from the Real Time & historical services in the DSS
- Real Time/historical servers receive replicated data from the operational environment

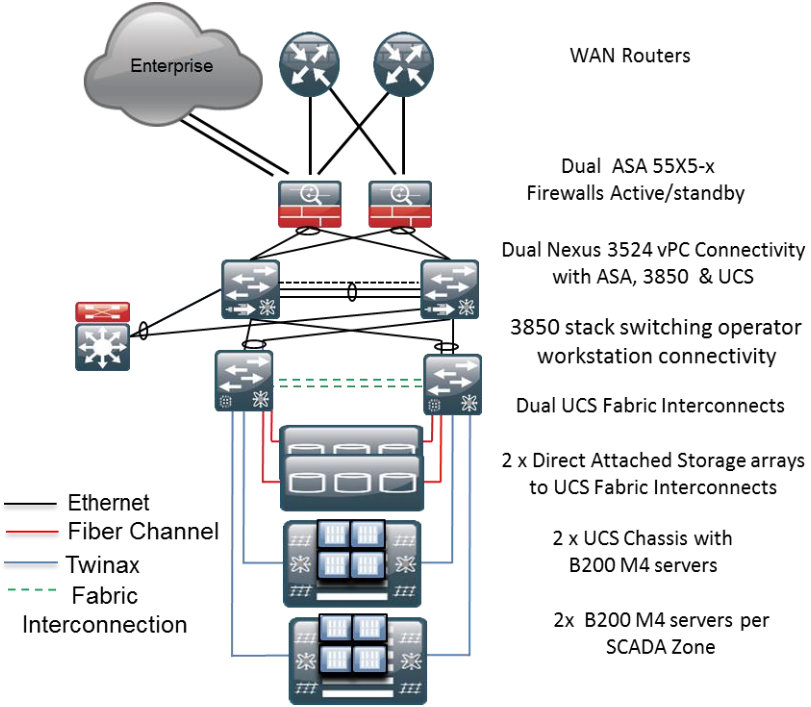

Levels 4-5
User
ezXOS Client
ENTERPRISE
RCS Service with Authorized Users
Level 3.5
IDMZ/ DSS
Remote Access Servers, RCS & RDP
Replication to DSS from Real Time and Historical
Levels 1-3
SCADA ZONE
SCADA Servers
Cisco ASA

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

Availability Overview

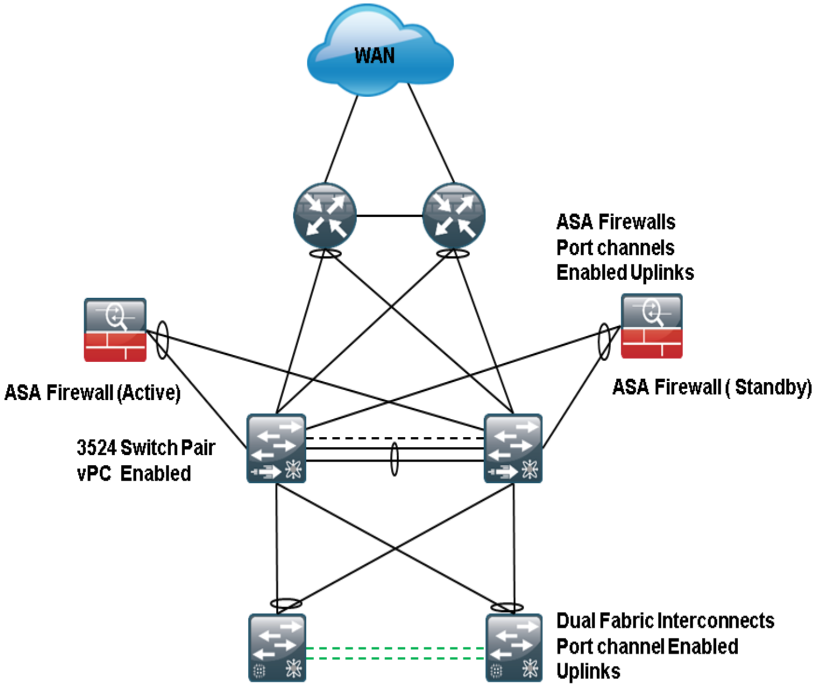
Resource Availability (RA) (ISA-62443-3-3 FR 7)

- No Single Point of Failure of any critical system component of the SCADA system, 24/7/365
- Dual servers for all critical components
- Application redundancy, Constant update of information between hot/standby apps and servers
- Redundant networking platforms, including routers, switches, firewalls, & Fabric Interconnects
- Storage redundancy RAID, controller, and chassis redundancy where appropriate, Dual SANs
- Redundant data paths across the network
- QoS prioritization of key network traffic and data


Enterprise
WAN Routers
Dual ASA 55X5-x Firewalls Active/standby
Dual Nexus 3524 vPC Connectivity with ASA, 3850 & UCS
3850 stack switching operator workstation connectivity
Dual UCS Fabric Interconnects
2 x Direct Attached Storage arrays to UCS Fabric Interconnects
2 x UCS Chassis with B200 M4 servers
2x B200 M4 servers per SCADA Zone
Ethernet
Fiber Channel
Twinax
Fabric Interconnection

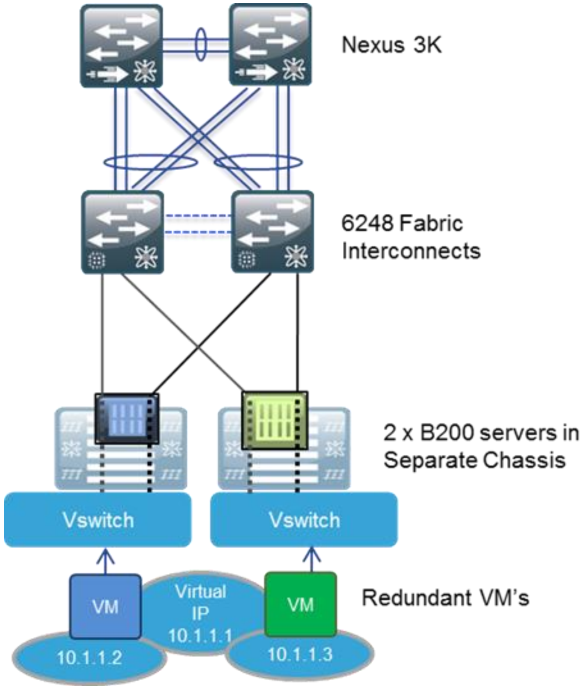
Network Availability

- Link and Platform redundancy at all levels
- Link aggregation and resiliency enabled with port channels and vPC
- Redundant ASA Firewalls Active/Standby



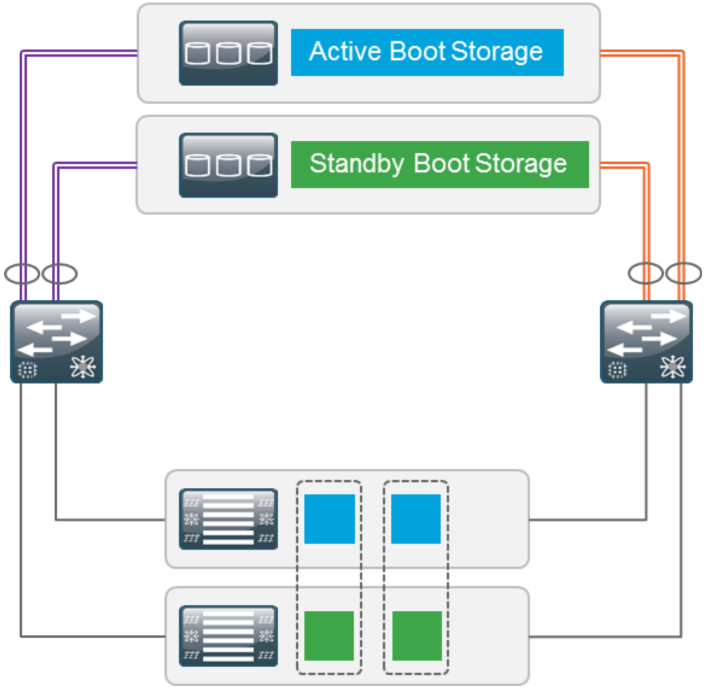
SCADA Server Connectivity and Redundancy (Virtual Machines)

- Two Separate Physical Servers providing Redundancy per Environment (Production, Test, DSS)
- Fabric Redundancy Enabled
- Virtual IP shared between Redundant Servers for SCADA Communication to the pipeline
- Active/Standby VM/Guest pair
- Application driven redundancy; SCADA Server redundancy decision at the application layer



Storage Redundancy

- Dual port adapters per host. Dual Storage controllers
- Two Storage Chassis directly connected to redundant fabric interconnects
- Servers boot from SAN
- OS and storage are mapped to specific hosts to ensure physical redundancy and dedicated server resources
- Raid 1 hardware mirroring
- 2 node clustering Microsoft SQL Database configured for the historical servers redundancy

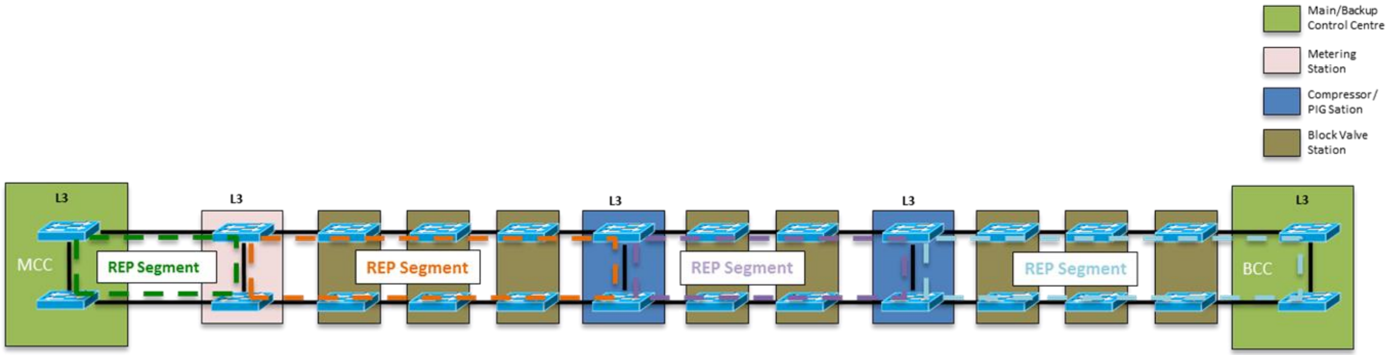


Design & Implementation – Pipeline Operational Telecom Network

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

Technology Options

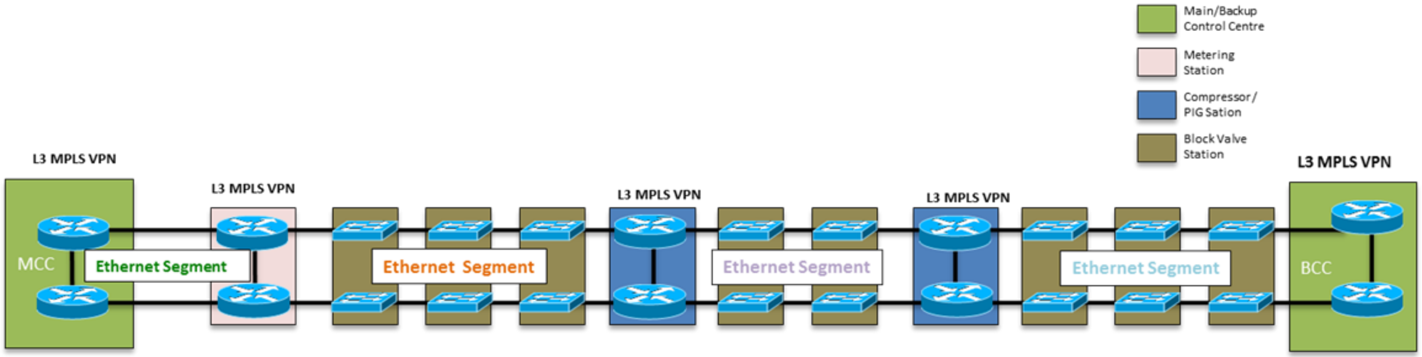
Ethernet



- **Segmentation:** Layer 2 VLANs allow for logical segmentation of operational and non-operational services over the same physical infrastructure.
- **Availability:** Resilient Ethernet Protocol (REP) for ring topologies re-convergence times of 50ms. Layer 3 routing protocols and VPNs provide reachability to the Ethernet segments over a core infrastructure.
- **Multi-Service:** Flexible QoS, allows operators to prioritize operational above non-operational services over a single infrastructure
- **Distance:** The distance between stations is 80 km maximum

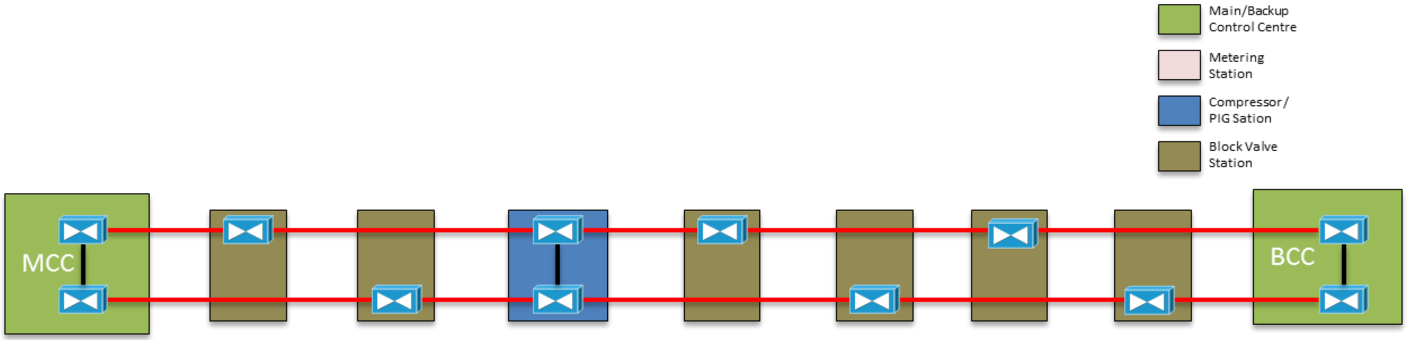
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

MPLS



- **Segmentation:** Logical proven security through Layer 2 or Layer 3 VPNs
- **Availability:** Traffic path selection on a per-application, MPLS FRR mechanisms (for network convergence <50 ms), traffic engineering to provide deterministic application flow
- **Multi-Service:** MPLS supports a flexible QoS, allowing operators to converge and prioritize operational above non-operational services
- **Distance:** The distance limitation between stations is 80 km maximum

DWDM



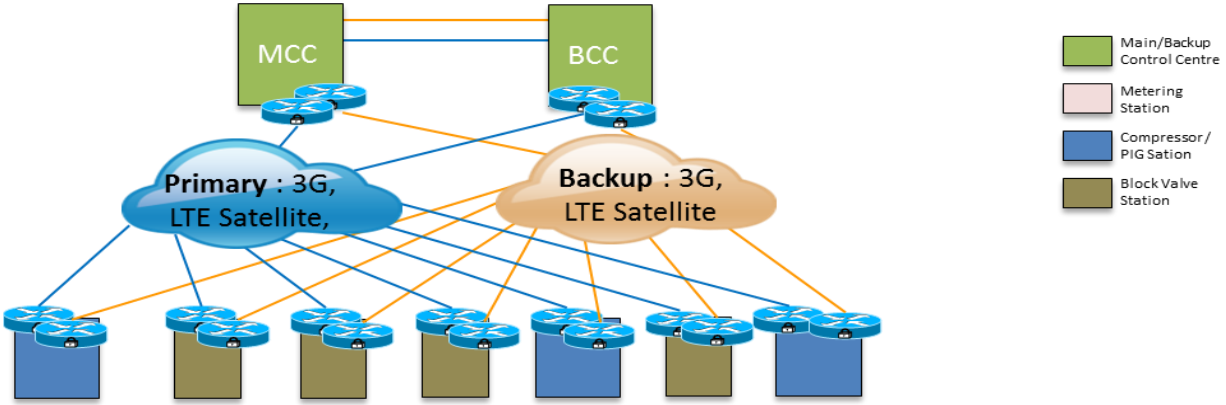
Segmentation: End-to-end proven security options through wavelength/lambda **separation** for service separation

Availability: sub-50 ms path protection. Amplification and error correction capabilities provide a more reliable transmission media over longer distances.

Multi-Service: Transparently carry IP, MPLS, and Ethernet technologies, as well as TDM.

Long-distance Connectivity: With amplification and error correction, the transmission capacity can be extended to 1000s of KM

Wireless/3G/4G


MCC
BCC
Primary : 3G, LTE Satellite,
Backup : 3G, LTE Satellite
Main/Backup Control Centre
Metering Station
Compressor/ PIG Sation
Block Valve Station

Brownfield deployments or where fiber is not available, Deployable as a backup to wired technologies

Security: VPN services and encryption over public infrastructure

Availability: Primary and backup baths using alternative technologies or service providers per site

Multi-Service: Bandwidth is limited QoS is essential to ensure prioritization of operational over non operational services

Operational Telecommunications - Validated Design

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

Operational Telecoms Network Overview

Core MPLS Network

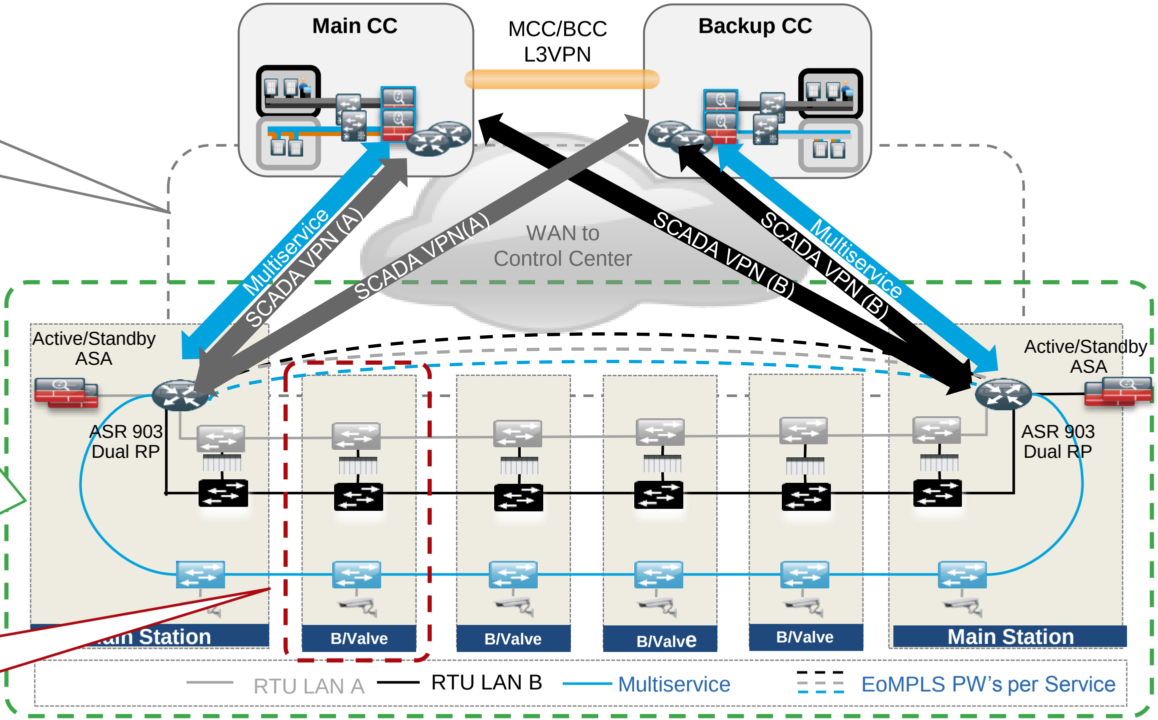
- L3VPN Service between the CC and pipeline
- Customer owned

Pipeline Telecom

- Optical fiber along the pipeline
- L2 Ethernet rings between Main stations
- Dual SCADA networks
- Separate Multiservice Ring
- L2.5 Routed firewalls to enforce security at protected subnets

Station Network

- Station RTU's Dual connected to each SCADA network



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

Security Overview

In a Pipeline architecture, the ability to securely restrict and isolate services to protect the integrity of the traffic is paramount. Intentional or accidental cross pollination of traffic between untrusted entities must be restricted

- Promote path isolation techniques both physical and logical to promote a dedicated infrastructure per service. VLANs, L3VPN instances, physically separated interfaces of equipment and security policies
  - *Restricted Data Flow (RDF) (ISA-62443-3-3 FR 5)*
- At routed boundaries, firewalls, ACLs, should be implemented to prevent cross pollination of traffic between services and provide isolation between zones
  - *Restricted Data Flow (RDF) (ISA-62443-3-3 FR 5)*
- Provide an auditable trail of security events.
  - *Timely Response to Events (TRE) (ISA-62443-3-3 FR 6)*
- With logical association of firewalls, VLANs, L3VPN instances, physically separated interfaces of equipment and security policies, a perimeter can be defined adhering to requirements of IEC 62443.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

Availability Overview

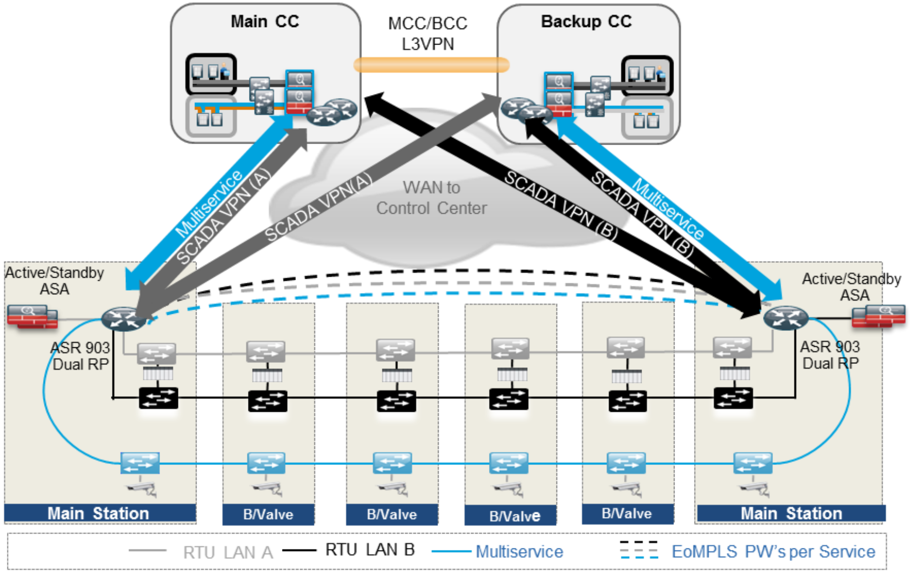
- *Resource Availability (RA) (ISA-62443-3-3 FR 7)*
- 24/7/365 control. Highly available communications network is essential to support the control and operations of the pipeline.
- Dual SCADA networks, Platform redundancy, network & path redundancy. Promote redundancy at all aspects of the architecture.
- Recovery from "dual" fiber cuts is a common requirement. Fiber pairs may be multiple but still within the same "Physical" failure domain such as a single conduit.
- Prioritize operational communications. Enable QoS throughout the architecture
- Security and safety is tied heavily to availability.

Operational Telecoms Pipeline Communication Flows

- SCADA Control center <-> pipeline communications
  - Modbus-TCP
  - DNP3

- Inter Control Center communication to allow replication between Primary and standby SCADA systems

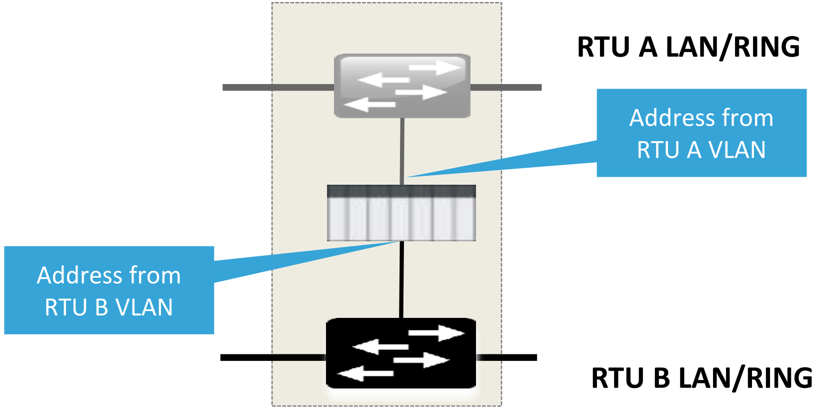
- Inter station communication between RTU's for peer to peer communication



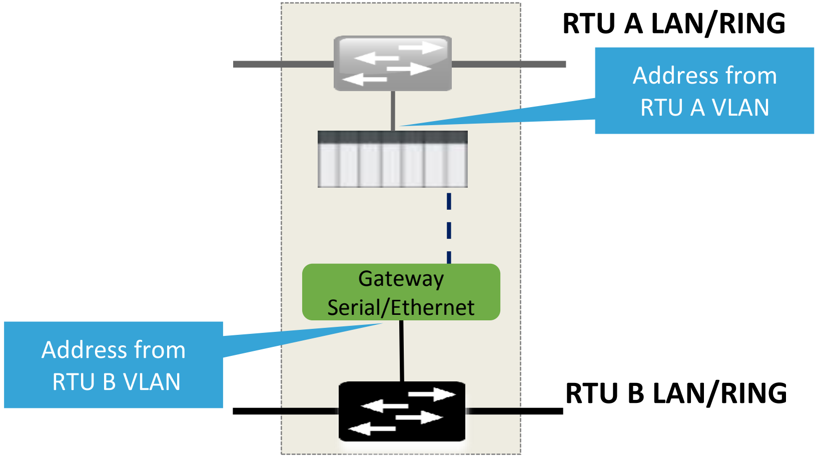
Cisco live!

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

RTU Availability Dual Ethernet Networks



- Single RTU dual Ethernet interfaces
- Separately addressable Ethernet interfaces and VLANS
- Both ports are active and can communicate with the Control Center



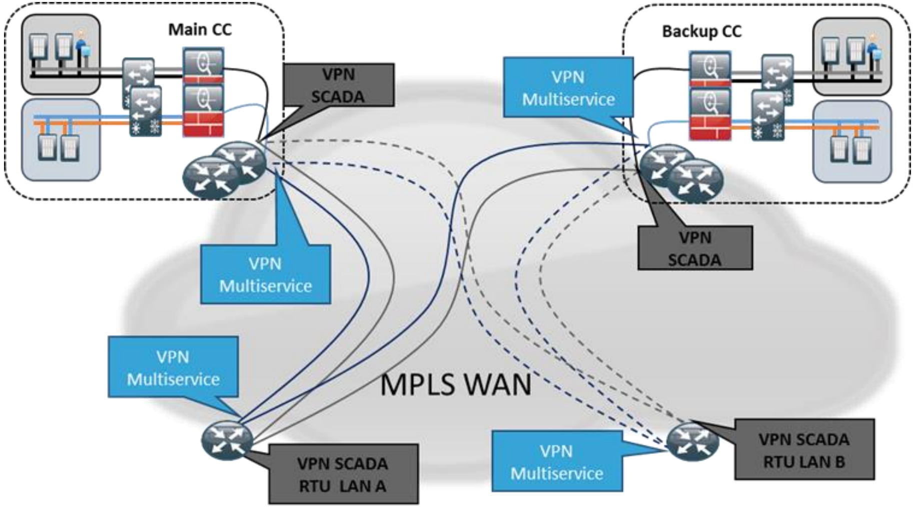
- Single Ethernet controller with serial /Ethernet Gateway

Dual connected SCADA devices provide greater flexibility with the availability design

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

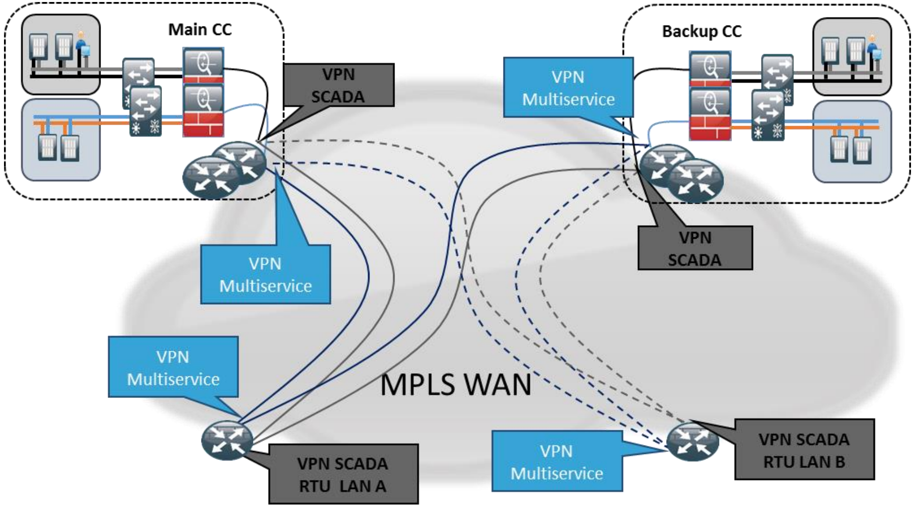
Core MPLS Availability

- Connectivity to the SCADA RTU's via two separate L3VPN's
- Each SCADA RTU network for a segment is terminated at different main stations…
- QoS prioritizes SCADA communications over all other traffic
- Loop Free Alternate (LFA) and Remote LFA (rLFA) Fast Re Route(FRR) are used for unicast MPLS/IP traffic
- L3VPN configured in BGP.. BGP Prefix Independent Convergence throughout the system for re-convergence within 100ms



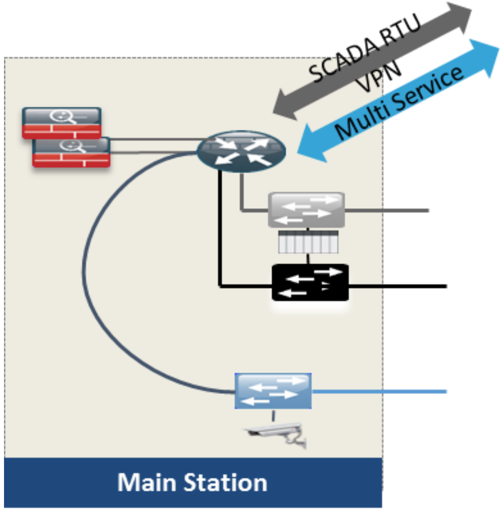
Core MPLS Security

- Company maintained Core network modelled for the CVD
- Encryption best practice if over a public infrastructure
- MPLS L3VPN provide logical segmentation of services between SCADA and multiservice networks



Routing/Layer 3 Availability

- ASAs are layer 3 gateway for each instance of the SCADA networks at each main station.
- Enforces policy, isolation and prevent cross pollination of traffic at a routed boundary
- Active Standby ASA Pair
- Routing is enabled between the ASA and the VRF instance on the ASR router

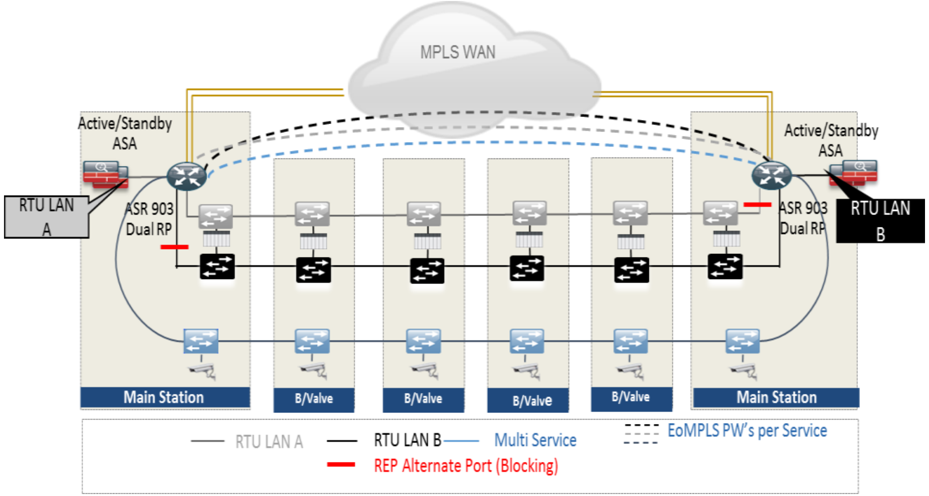


Pipeline segment Availability SCADA

- ASA L3 gateway for SCADA
- Separate RTU SCADA A and B networks
- Each SCADA RTU network for a segment is terminated at different main stations
- L2 Ethernet Rings along a segment between two main stations
- Resilient Ethernet Protocol (REP) provides fast convergence within the L2 domains for the L2 rings
- Two Validated models

  EoMPLS Pseudo wire ring closure

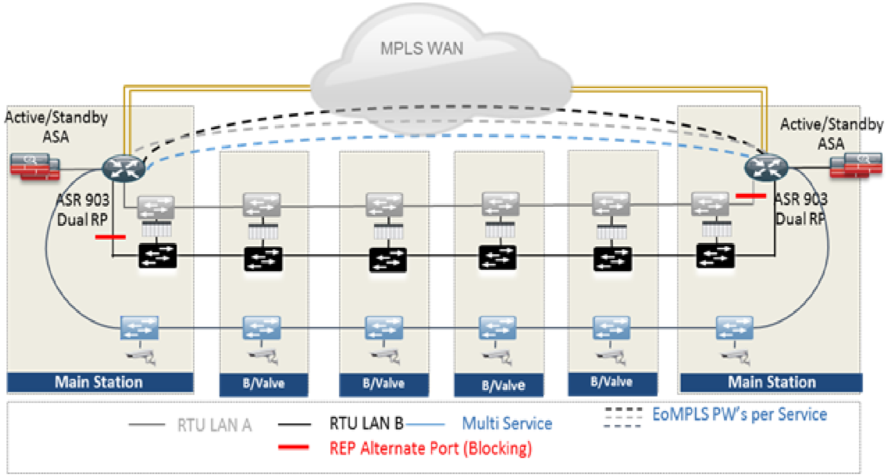
  Alternate station Hopping



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

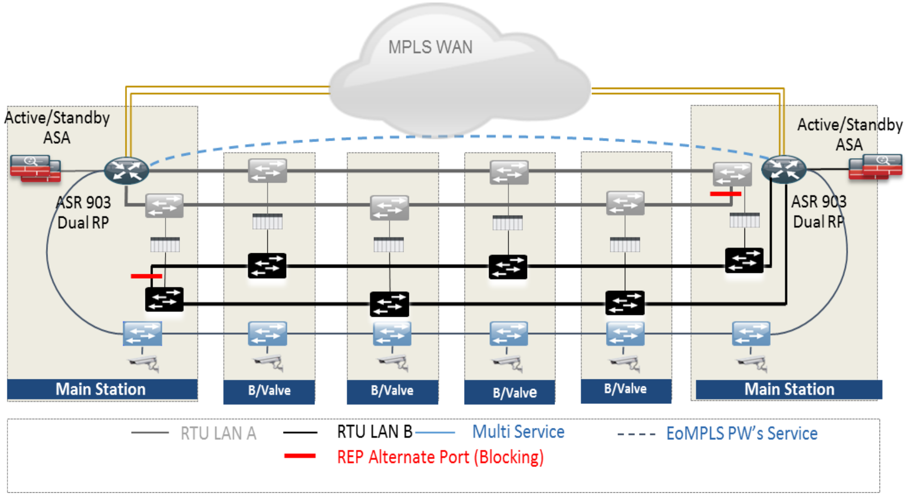
EoMPLS Pseudo Wire Ring Closure

- EoMPLS PW extend the layer 2 domain between the main stations to close the rings
- Deployed where distance between main stations is a factor or Fiber strands may be limited
- Designed so that EoMPLS tunnel is only used under failure conditions



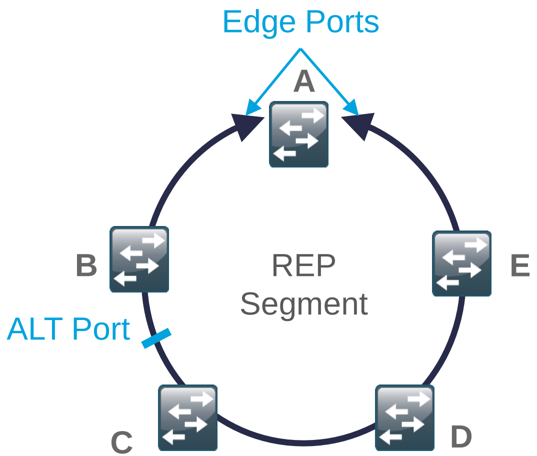
Alternate Station Hopping

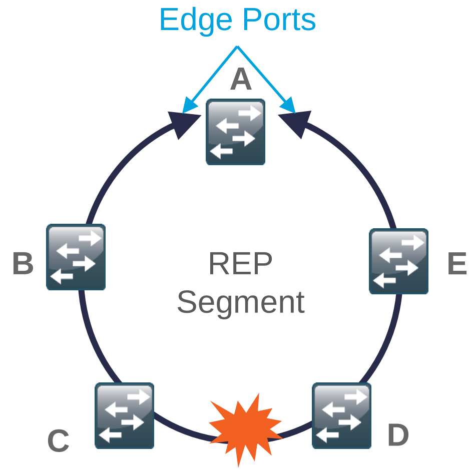
- Connectivity between alternate stations and loops the ring at the far end station
- Multiple fiber cut would prevent connectivity between stations either side of the break
- Control center would still have connectivity to all stations on at least one of the RTU LANs
- EoMPLS PW design would circumvent this



REP Overview

- REP provides a way to control network loops, handle link failures, and improve convergence time in the range of 50 -200 ms
- A REP segment is a chain of ports connected with the same segment ID
- One switch can only have two ports in the same segment
- Edge ports terminate the REP segment
- When all interfaces in the segment are up, the alternate port is blocking
- When a link or switch failure occurs, the blocked alternate port begins forwarding

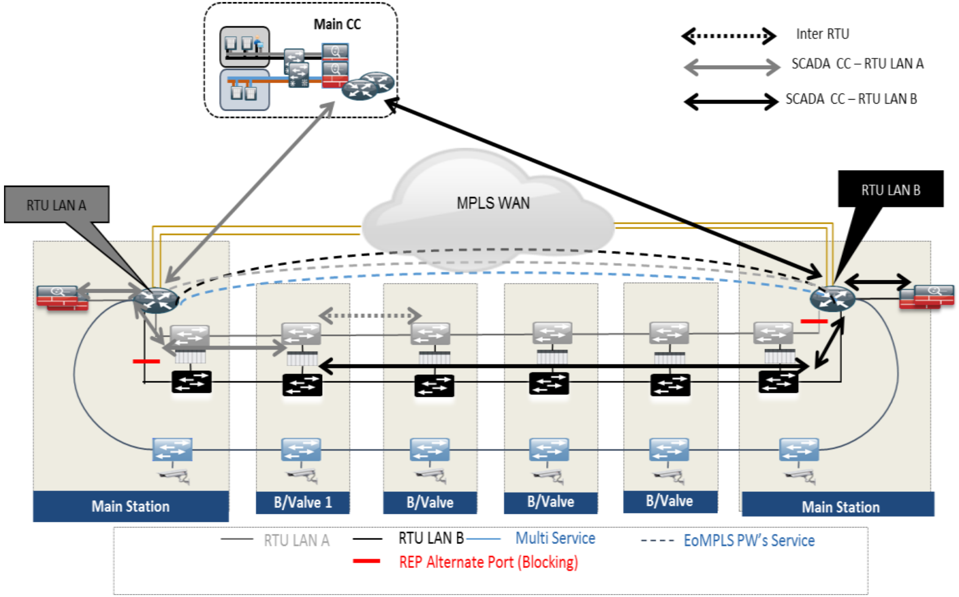




© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

Resilient Ethernet Protocol

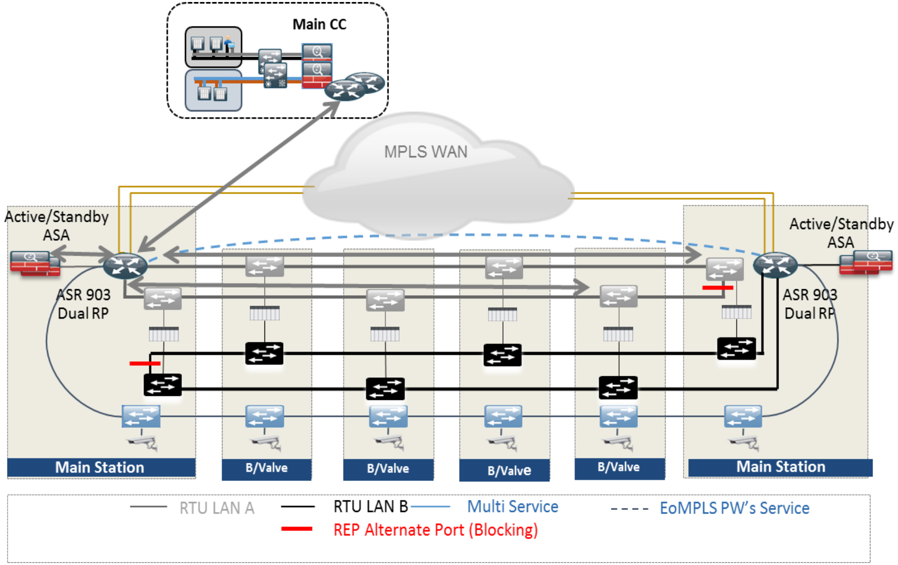
- REP alternate ports at opposing stations to L3 gateway,
- Only use the EoMPLS in failure scenarios
- On fault restoration the Alternate port (by default) will return to the place of the failure
- **Preemption should be configured** to return the Alternate blocking port to the opposing station



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

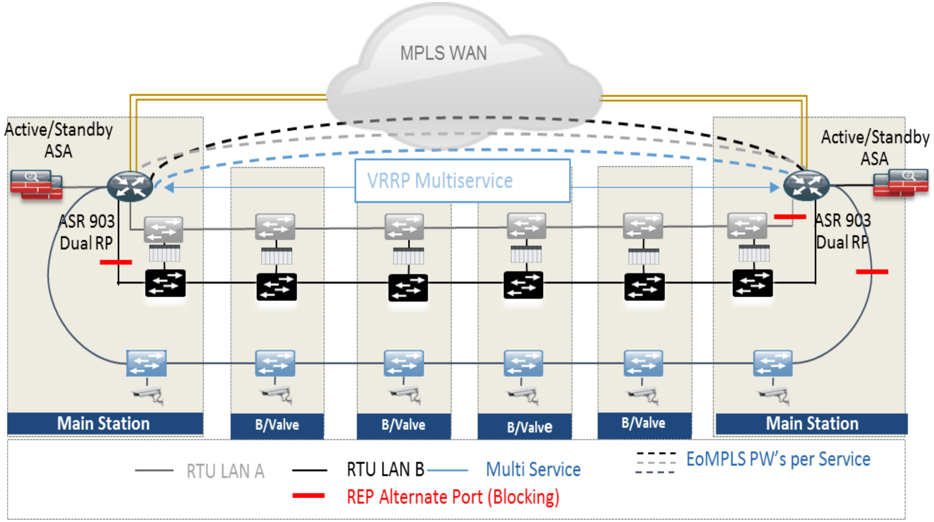
Resilient Ethernet Protocol

- REP alternate port is placed at the midpoint in the ring
- Optimize path diversity for Control Center to RTU communications
- Restrict the number of switches the traffic must traverse during normal operations



Pipeline Telecom Availability Multiservices

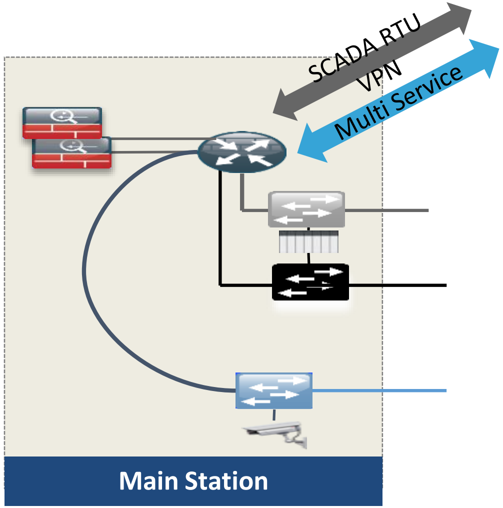
- Multiservice end points will not be dual attached as per the RTU's
- Virtual Router Redundancy Protocol (VRRP) will run between the two ASR's
- The multi services rings will be running REP
- Multiservice ring will be closed using an EoMPLS pseudo wire
- The Alternate port will be configured on the non VRRP active ASR



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

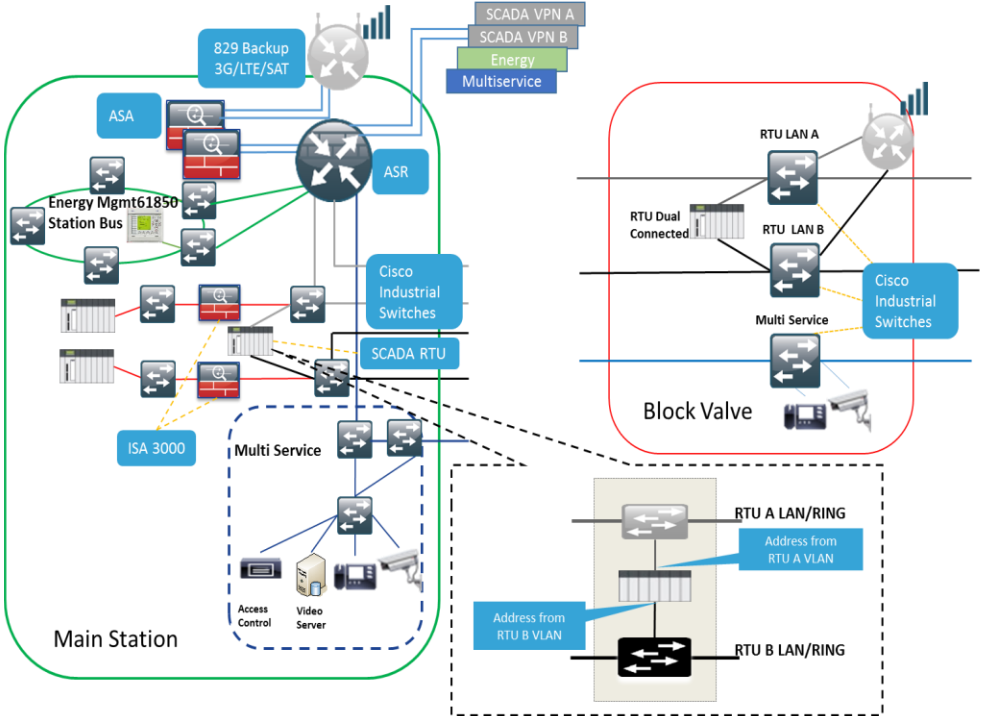
Pipeline Telecom Security

- Networks physically segmented using L2 Rings
- ASAs are layer 3 gateway for each instance of the SCADA networks at each main station
- Inter zone security protects the SCADA RTU LANS
- Policy and security point between pipeline segments and inter-pipeline security.
- ACL's applied at the ASR routers to restrict access to Multiservice network
- QoS enabled to help police for oversubscription and anomalous behavior
- Control Plane Policing (CoPP) at the ASR Routers



Pipeline Station Overview

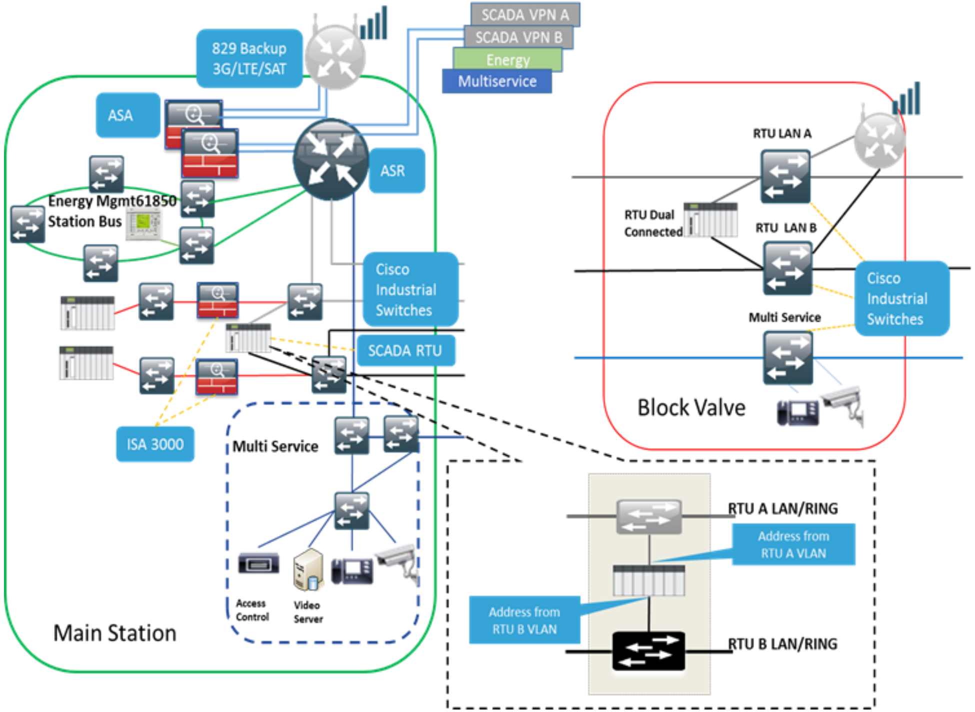
- Physical Segmentation of Networks
- Level 2.5 Firewalls in the main station
  - Station protection, inter-zone security (process control, safety system, energy)
- Inter zone security protecting the SCADA RTU LANS
- Standard switch based security such as
  - Shutdown unused ports. Port Security, Traffic Control



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

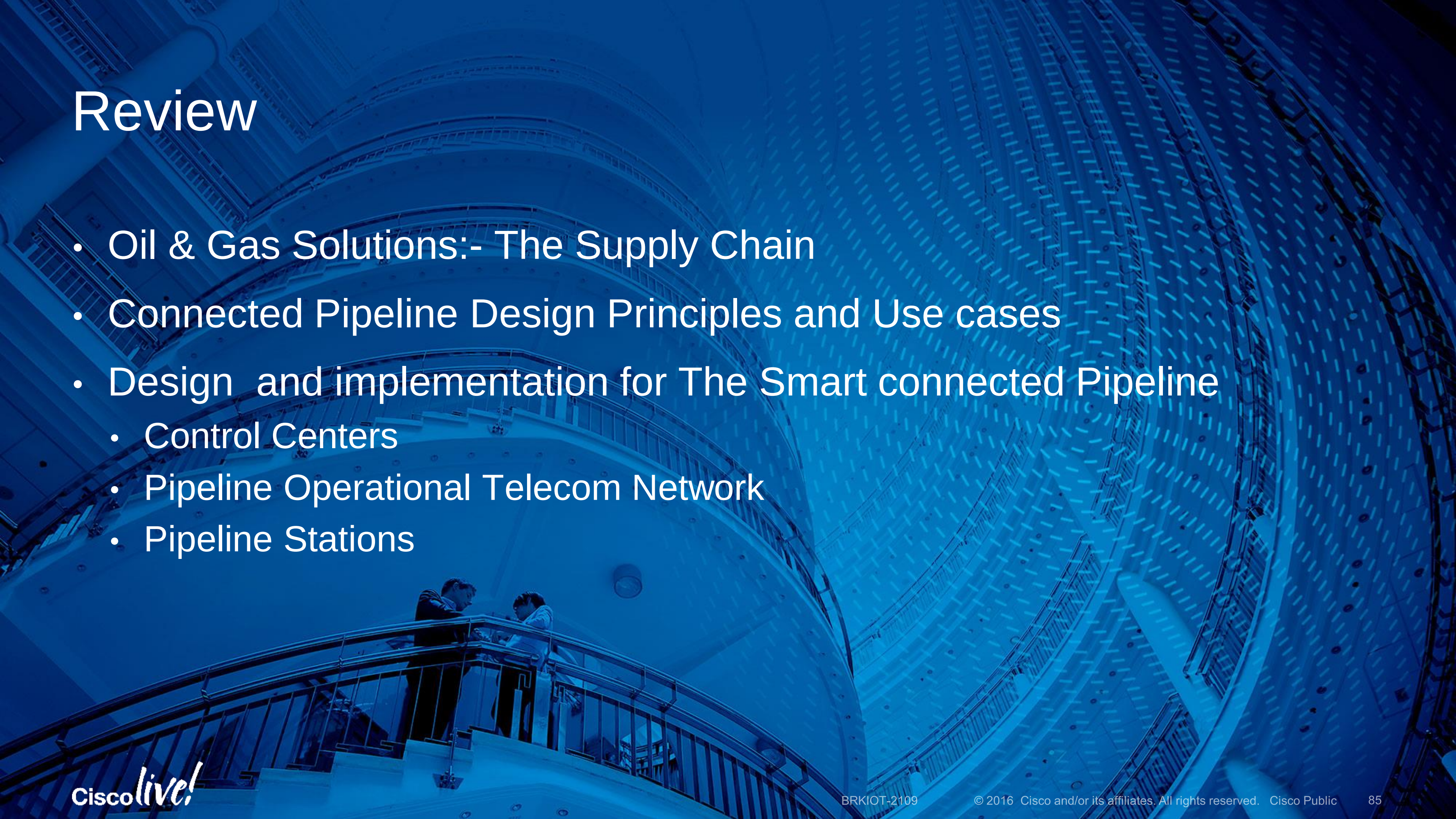
Pipeline Station Overview

- Dual RTU Connectivity
- IE Switches REP enabled
- 829 Backup Router, encrypted transport over public infrastructure, Zone Based Firewall if required



Pipeline Integrated Network Management

- Present visibility of infrastructure alarms, events and networking statistics to the pipeline operator
- Syslog and SNMP are the mechanisms to report to a fault management system which presents the notification to an operator
- Enforce secure use of network management traffic (SSH, SNMP v3)
- Role Based Access Control (RBAC)
- Out Of Band Management Where possible if not dedicated VLAN
- Cisco Prime Infrastructure delivers a single, unified platform for network service provisioning, monitoring and assurance and change and compliance management. IE switches, ASR 903
- ASDM allows the user to configure, monitor, and troubleshoot Cisco firewalls
- Cisco UCS Manager provides an intuitive GUI, a CLI, and a robust API to manage all system configuration and operations

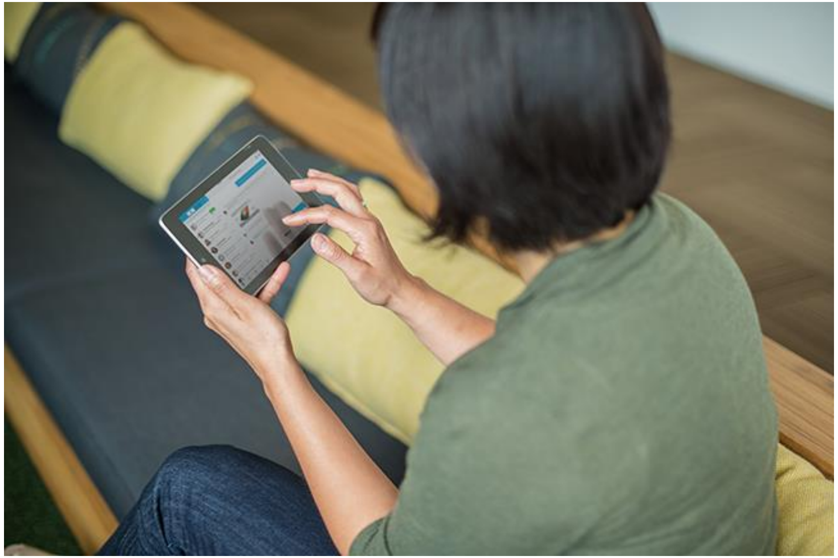


Review

- Oil & Gas Solutions:- The Supply Chain
- Connected Pipeline Design Principles and Use cases
- Design and implementation for The Smart connected Pipeline
  - Control Centers
  - Pipeline Operational Telecom Network
  - Pipeline Stations

Complete Your Online Session Evaluation

- Give us your feedback to be entered into a Daily Survey Drawing. A daily winner will receive a $750 Amazon gift card.
- Complete your session surveys through the Cisco Live mobile app or from the Session Catalog on CiscoLive.com/us.



Don't forget: Cisco Live sessions will be available for viewing on-demand after the event at CiscoLive.com/Online

Continue Your Education

- Demos in the Cisco campus
- Walk-in Self-Paced Labs
- Lunch & Learn
- Meet the Engineer 1:1 meetings
- Related sessions

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

Please join us for the Service Provider Innovation Talk featuring:

Yvette Kanouff | Senior Vice President and General Manager, SP Business

Joe Cozzolino | Senior Vice President, Cisco Services

Thursday, July 14th, 2016

11:30 am - 12:30pm, In the Oceanside A room

What to expect from this innovation talk

- Insights on market trends and forecasts
- Preview of key technologies and capabilities
- Innovative demonstrations of the latest and greatest products
- Better understanding of how Cisco can help you succeed

Register to attend the session live now or watch the broadcast on cisco.com

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

Thank you

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco live!

July 10-14, 2016 • Las Vegas, NV

Internet of Things (IoT) Cisco Education Offerings

Course	Description	Cisco Certification
NEW! IMINS2	An associate level instructor led training course designed to prepare you for the CCNA Industrial certification	CCNA® Industrial
Managing Industrial Networks with Cisco Networking Technologies (IMINS)	This curriculum addresses foundational skills needed to manage and administer networked industrial control systems. It provides plant administrators, control system engineers and traditional network engineers with an understanding of the networking technologies needed in today's connected plants and enterprises	Cisco Industrial Networking Specialist
Control Systems Fundamentals for Industrial Networking (ICINS)	For IT and Network Engineers, covers basic concepts in Industrial Control systems including an introduction to automation industry verticals, automation environment and an overview of industrial control networks	
Networking Fundamentals for Industrial Control Systems (INICS)	For Industrial Engineers and Control System Technicians, covers basic IP and networking concepts, and introductory overview of Automation industry Protocols.	

For more details, please visit: http://learningnetwork.cisco.com
Questions? Visit the Learning@Cisco Booth or contact ask-edu-pm-dcv@cisco.com

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public