Cisco IoT

Cisco Digital Utilities: Prozesskommunikationsnetze in der Energieversorgung

Volker Sorhage

KBC Forum – 09.11.2023

Utilities face unique challenges

The need for agility is accelerating their digitization

New demands on the network

Digitization isn't easy

- More devices, more bandwidth
- Cyber Security
- More capabilities in a smaller footprint
- Zero-touch-Deploy and Manage at Scale
- Highly resilient networks
- IEC 61850 & Precision timing

Cisco IoT

Utility networks can benefit from enterprise capabilities

Helping to avoid:

Less secure, unsegmented

Evolving threats

Air gapped, unsegmented or flat Layer-2 networks

Lack of asset visibility

Complexity at scale

Multiple vendors and networks

Multiple touch points

Multi-step, complex interactions

Difficulty resolving issues

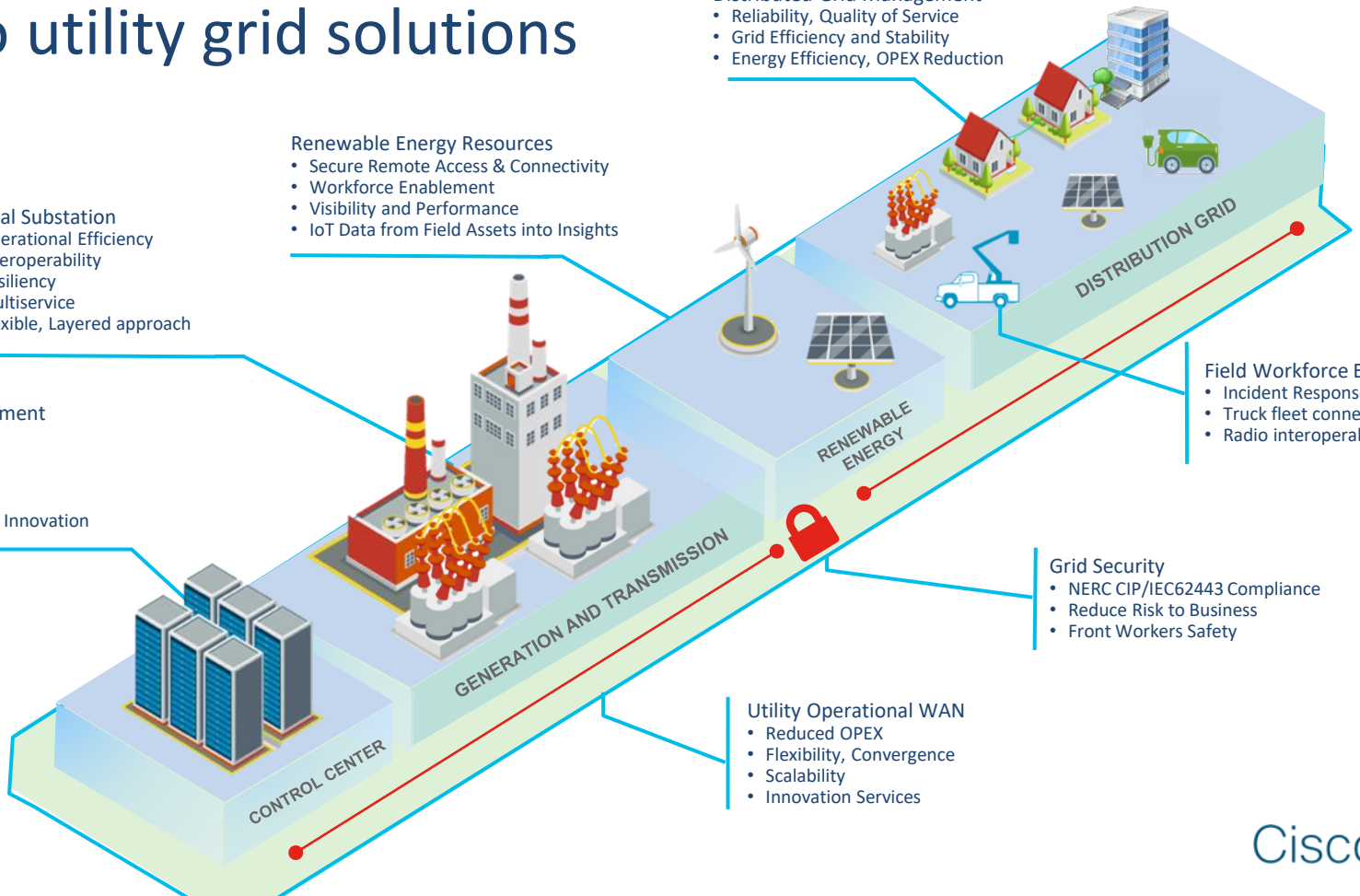
Poor network visibility

Long outages due to reactive troubleshooting

Manual processes

Talent shortages compound the issue – IT/OT need enterprise capabilities to keep up

Cisco utility grid solutions



Cisco IoT

Four main pillars for Cisco utility grid solutions

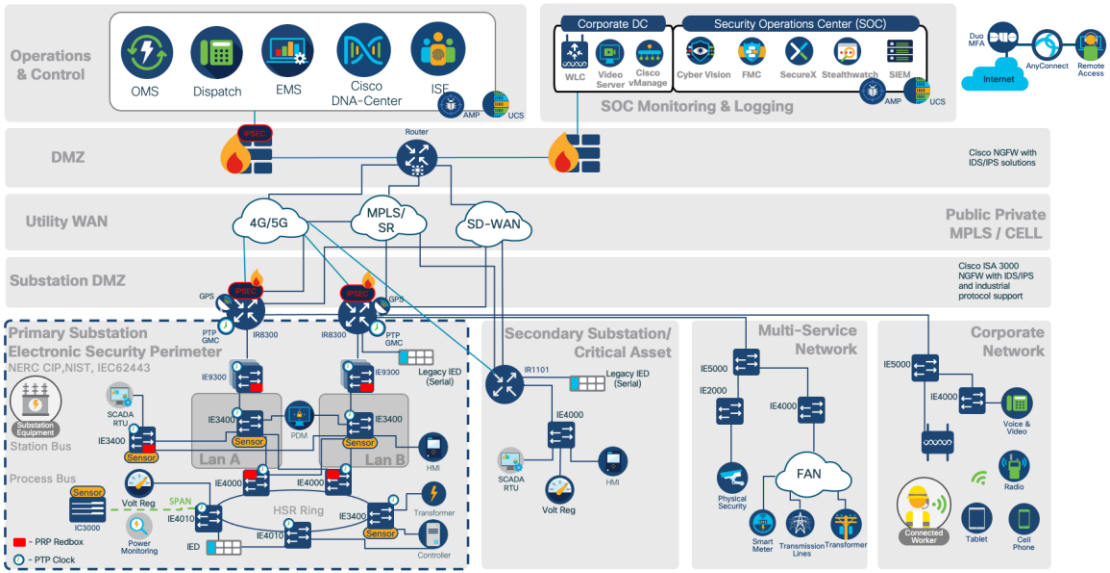
- Cisco Validated Designs
- OT Ready HW & SW Based on IT Technology
- Build In Security
- Management at Scale

Cisco IoT

Cisco Validated Design: Substation Automation

Modernize Grid operations

Foundation for advanced protection and control, remote diagnostics and predictive maintenance capabilities.



Outcomes

- Grid Modernization and sustainable energy
- Reduce operational cost and increase reliability
- Reduce risk from cybersecurity threats

Features/Functions

- Support SCADA - Serial/TDM to IP transition and Station & Process bus systems – (IEC 61850 compliance, DNP3)
- Support Tele-protection and power management (Synchorphasor/PMU, Volt/Var) applications
- Cybersecurity support for NERC CIP compliance
- Visibility of substation devices and communications
- Support lossless network resiliency and precise timing
- Proactively identify WAN/LAN network issues and receive remediation suggestions and consistently configure and maintain network infrastructure

Benefits

- Validated Design and Implementation guidance developed by Cisco engineering
- Tested against leading substation vendor devices and applications
- Experienced Cisco services ready to apply to customer scenarios

Proven to work with: SEL Schweitzer Engineering Laboratories, SIEMENS, Schneider Electric, ABB

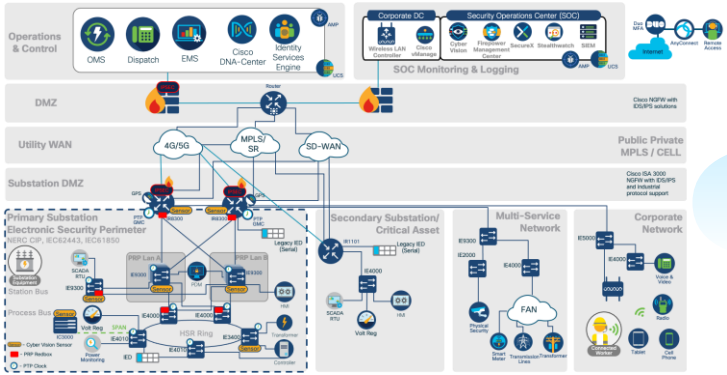
Cisco IoT

What's new in Substation 3.0

NEW

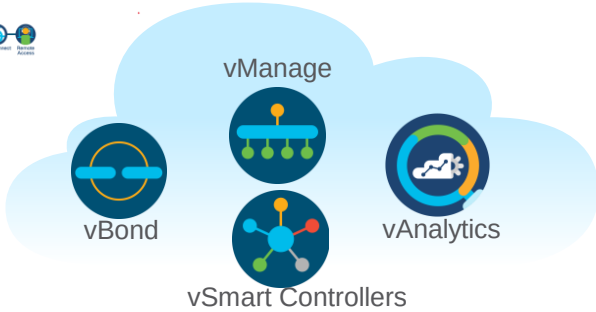
Cisco DNA Center & ISE for Substation LAN

Substation Automation CVD



NEW

Cisco SD-WAN for Utility Wide-Area Network



NEW

Catalyst IE9300 Rugged Series Switch

NEW

Catalyst IR8300 Rugged Series Router

Cisco Catalyst Switching Technology

Unleashing enterprise features at the industrial edge

IE-9300
26 SFP • 2 Combo ports
Redundant power supplies
Stackable

IE-3400
26 GBE • 2 Combo ports
DIN Rail Design
Redundant DC power
Edge Compute

Unrivaled performance at scale

- Up to 100 Gbps switching capacity
- 8x density with backplane stacking
- Unrivaled timing and synchronization: 50ns per hop PTP accuracy
- Better throughput: 5K TCAM entries

Unprecedented visibility of assets

- Endpoint and application visibility with Cyber Vision and NBAR2
- Better assurance: Full Flexible NetFlow and IOS-XE telemetry

Industry leading cyber security

- Operational vulnerability and security posture with Cyber Vision
- MACsec 256
- SD-Access fabric Edge and group-based policy (TrustSec)

Cisco IoT

Cisco Catalyst Routing Technology

Unleashing enterprise features at the industrial edge

IR1101
4 switch ports • SFP • 2combo WAN ports
Extension Module
PIM Design for 5G, LTE, LoraWAN, LTE450, Wifi 6...

IR8140
4 copper • 4 combo • 4 SFP • 2 combo WAN ports
4 expansion slots
5G • SD-WAN
Redundant power supplies
20x increased encryption*

Unrivaled performance at scale

- Single integrated platform for routing, switching and security
- Easier to manage: One control plane for Layer 2 and Layer 3
- Full MPLS Layer 3 support

Unprecedented visibility of assets

- DNA-Center and SD-WAN
- 8 core processor for dispersed workloads
- PoE, PoE+ and UPoE
- Backwards compatible with Serial
- Only Cisco router that converts GNSS time to NTP, PTP, SyncE

Industry leading cyber security

- Security and visibility with Cyber Vision
- Hardware based MACSec LAN and WAN
- IPSEC - DMVPN, FlexVPN, IKEv1, IKEv2
- URL filtering, Cisco AMP, Snort (IPS/IDS)
- Group based policy (TrustSec)
- Policy edge node support (DNA Center)
- Zone based firewall

* Encrypted throughput vs. previous generation

Cisco IoT

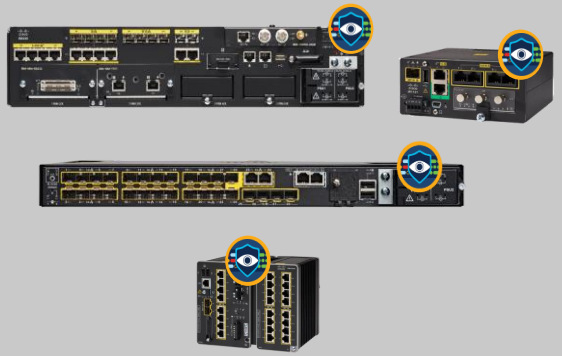
Cisco Catalyst IR1100 Rugged Series Routers

Cisco IoT

Gain **Operational Insights**

Cyber Vision Center
(Centralized analytics)

Application Flow

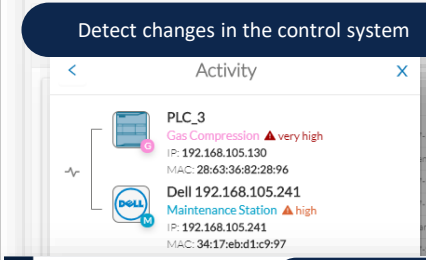


Network-Sensors
(Built in Deep Packet Inspection)

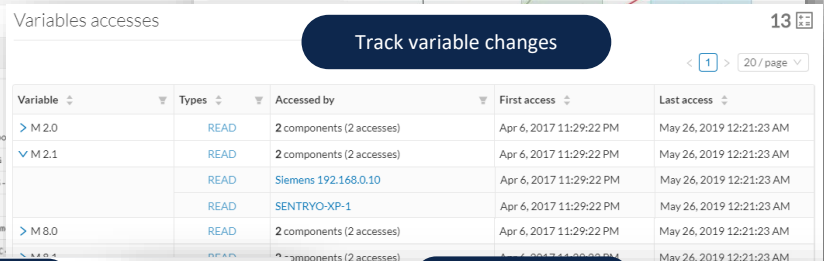
Comprehensive asset inventory

Dynamic communication map

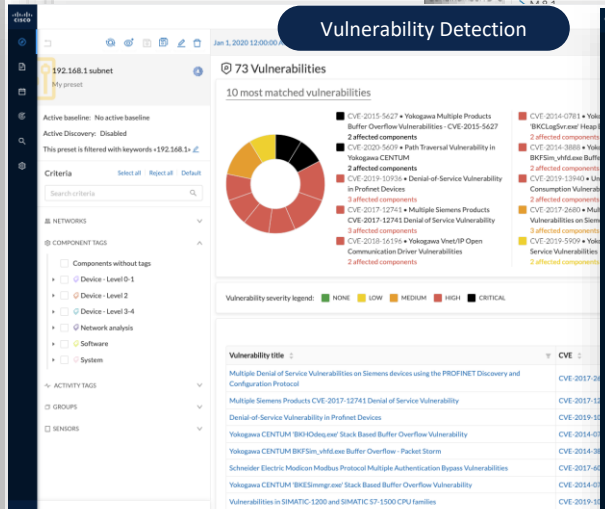
Detect changes in the control system



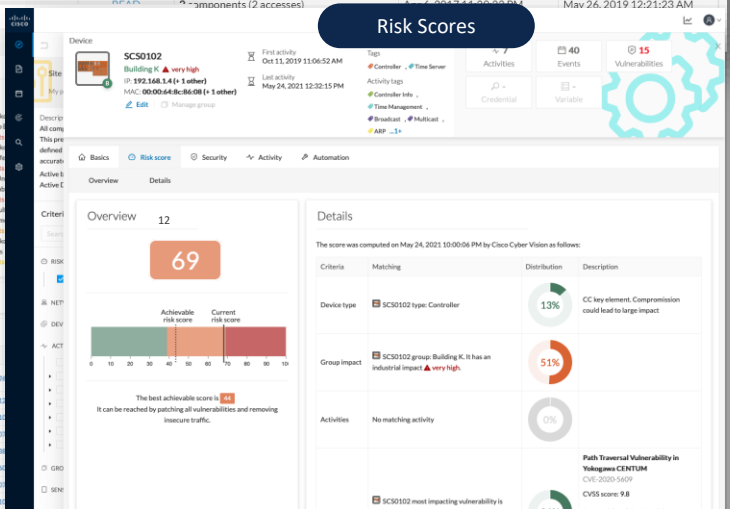
Track variable changes



Vulnerability Detection



Risk Scores

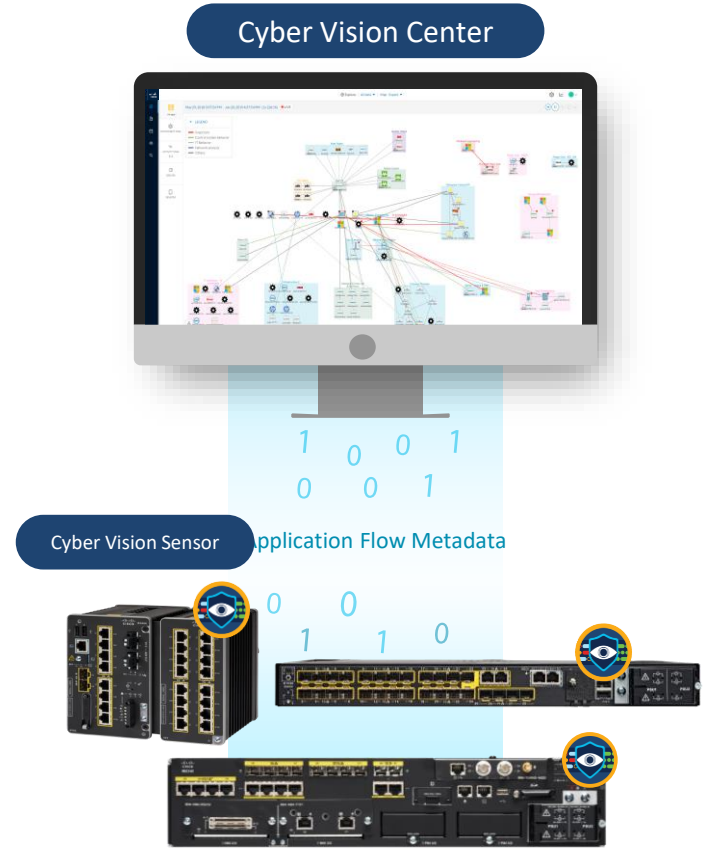


Visibility
Asset inventory
Communication patterns

Security Posture
Device vulnerabilities
Risk scoring

Operational Insights
Track process/device modifications
Record control system events

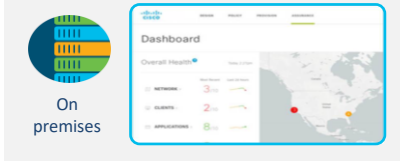
Cisco substation LAN switches and WAN routers **see everything** that attaches to them so you can gain **visibility at scale**



Deep Packet Inspection & Active Discovery
built into your network infrastructure

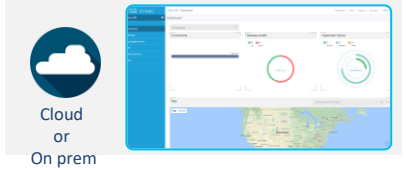
Utility Management Platform Selection

Cisco DNAC



Cisco FND

Cisco SDWAN



Substation Automation

- Integrated IT & OT network Management
- Routing & Switching
- Non-Fabric use case
- Assurance
- Compliance
- ZTD

Distribution Automation

- Cellular DA
- WiSUN Mesh
- Router + Endpoint management at scale
- No switching
- IoT features (Raw Sockets, Scada Translation)
- App management
- IPSEC Tunnel Automation
- PKI based ZTD

Substation & Distribution Automation

- WAN Router management
- IT Focused
- No WiSUN Mesh support
- No switching
- IPSEC Tunnel Automation
- PKI based ZTD

Cisco IoT

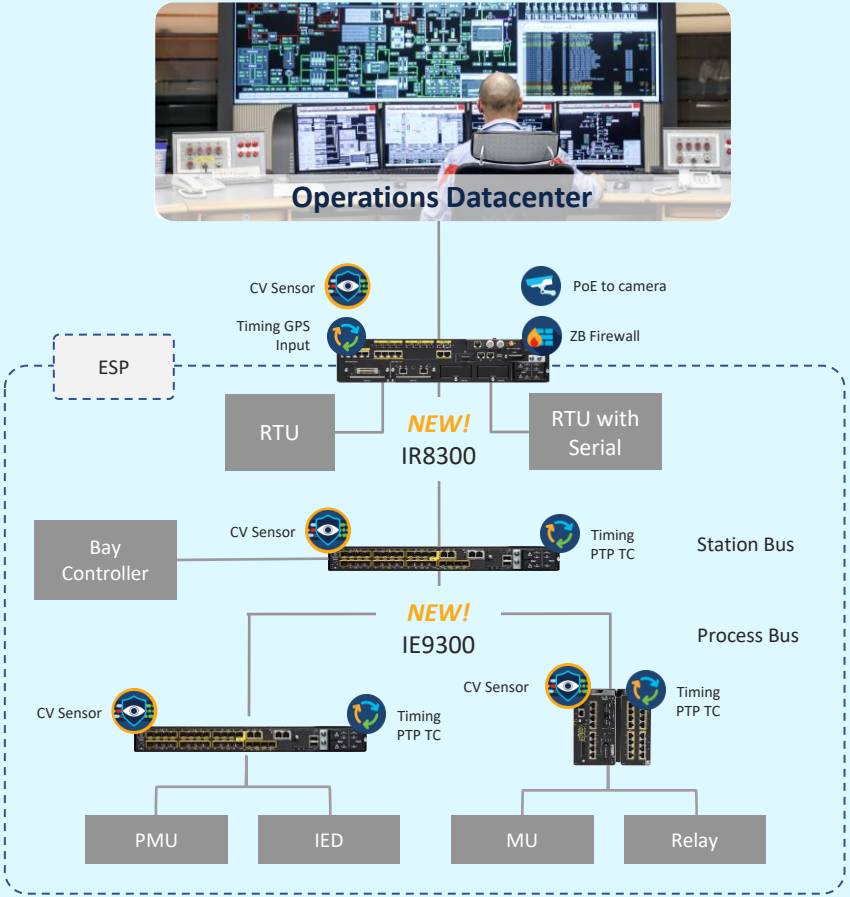
Key Takeaways
Cisco for Digital Utilities

- IT Infrastructure Ready for Digital Utilities
- Designs Validated and Proven in Use
- Future is Software Defined Infrastructure
- Industry-leading security built-in
- Management at Scale
- Cisco End–to-End Solution

Cisco IoT

The bridge to possible

Backup

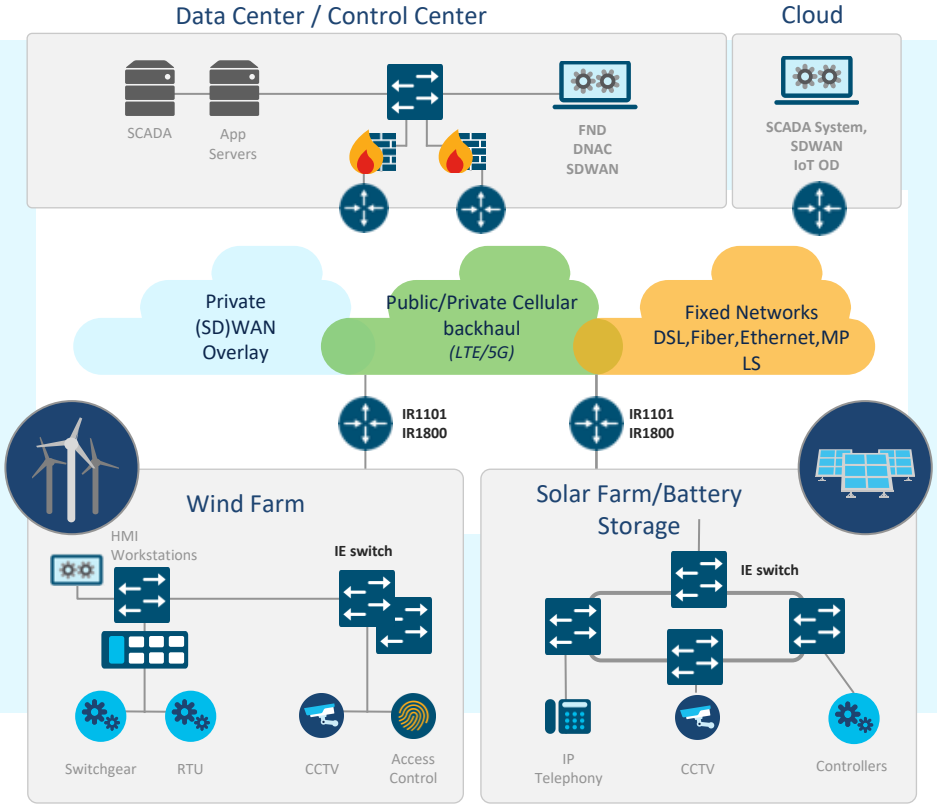


Secure turnkey communications for the modern Digital Substation

- **Support for all SCADA Services:**
  - Serial/TDM to IP transition
  - IEC61850 Station & Process bus architectures – (MMS,GOOSE & SV)
  - Support IEC104/DNP3 Architectures
- **Increased Throughput and bandwidth** – supporting more devices in the substation and bandwidth increases due to devices such as Synchro phasors/PMU and IP Cameras
- **Footprint Reduction** – More functionality in less boxes, PTP Timing, Resiliency (PRP,HSR), Security (Cybervision Sensor) reduces the Rack space, heat and power requirements.
- **Flexible WAN Gateway** – provides all the WAN connectivity requirements: MPLS, SDWAN, Cellular (Public & private 4/5G & Firstnet) with Encryption
- **Management and Automation** to proactively identify WAN/LAN network issues and receive remediation suggestions and consistently configure and maintain network infrastructure
- **Cybersecurity** – Help you achieve regulatory compliance via Asset Visibility & information plus product features.
- **Validated Architectures** – Designs tested and proven by Cisco to de risk deployments

Cisco IoT

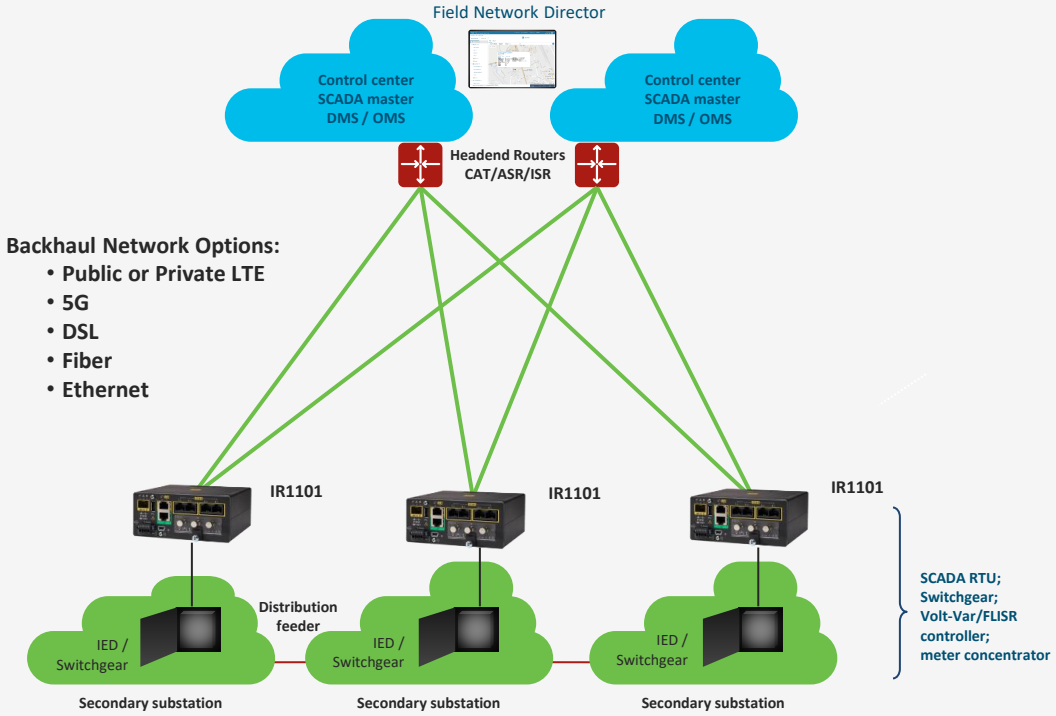
Distributed Energy Remote Sites



Design Considerations

- Applications:
  - Turbine Control & Monitoring
  - Battery/PV Inverter O&M
  - PV/battery Controller
- Components:
  - IR1101 (DSL, Serial Modules)
  - IR1800 (Wifi6,Unified Threat Defense for IDS)
  - IR8340 for larger sites
  - Management Choice IT vs OT
  - Cybervision for ICS visibility

Secondary Substation Solution



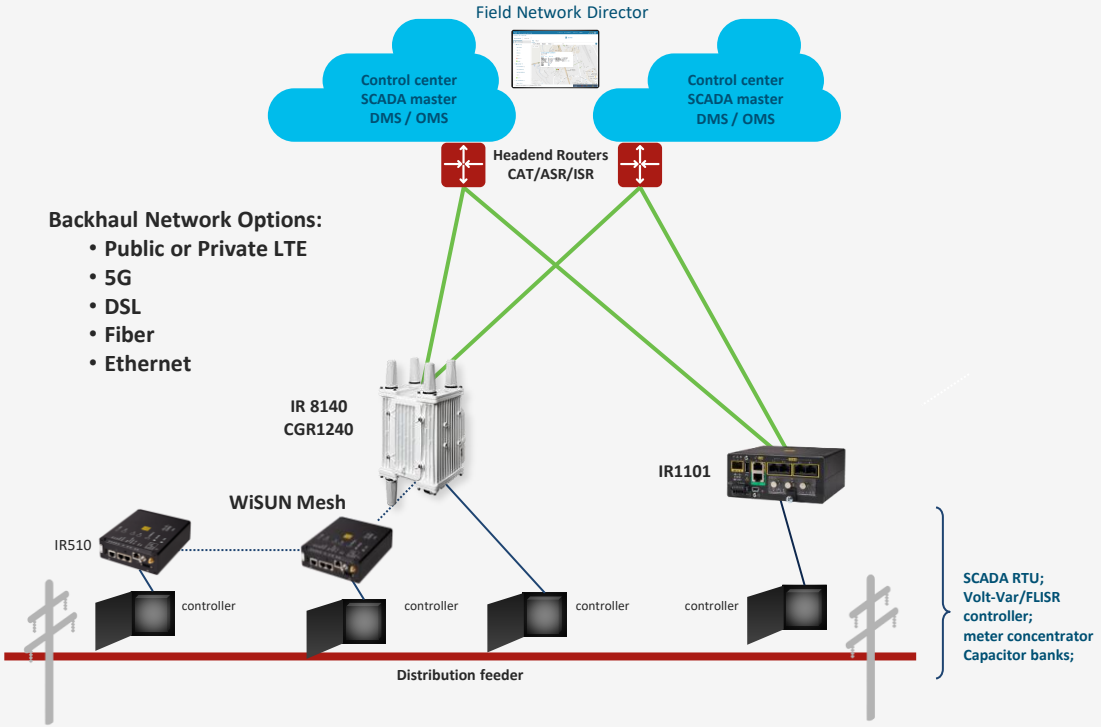
Applications:

- Volt-VAR control
- Fault location, isolation, and service restoration (FLISR) control
- Remote RTU & Switchgear
- Meter concentration
- SCADA transportation and gateway services: DNP3/DNP3-IP, IEC 60870-5-101/104, etc.
- Renewable Energy Integration

Components:

- Cisco® IoT gateway
  - IR1101
- Field area network (FND) management

Feeder Automation Solution



Applications:

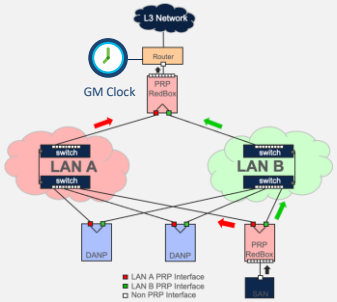
- Volt-VAR control
- Fault location, isolation, and service restoration (FLISR) control
- Remote RTU
- SCADA transportation and gateway services: DNP3/DNP3-IP, IEC 60870-5-101/104, etc.

Components:

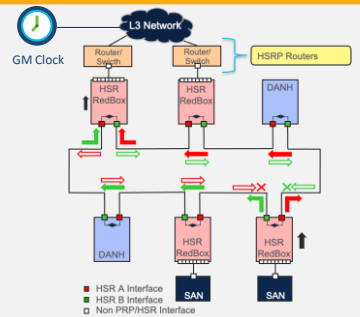
- Cisco IoT gateway
  - IR1101
- Cisco® Resilient Mesh
  - IR 8140
  - Cisco IR510, IR530
- Field Network Director (FND)

Support for IEC61850 on Process & Station Bus

Parallel Redundancy Protocol (PRP)



High-Speed Resiliency (HSR)



- Loss-less resiliency protocols and no single-point-of-failure topologies for maximum up-time
- Device Synchronization with **support for**
  - Power-Profile Precision Time protocol (Grandmaster, Transparent Clocks)
  - Wide-range of timing inputs and conversions
- Low-latency communications with Quality of Service settings to prioritize IEC61850 critical traffic
- IEC 61850 certifications for substation operations

Cisco IoT

Cisco Catalyst Industrial Networking Portfolio

Building a unified solution for IT and Operations

Enterprise grade + **Industrial grade**

Leverages existing IT knowledge and investments

- Industry-leading Cisco security end-to-end
- Less complexity at scale - one network
- Consistent software and licensing - IOS-XE
- Familiar tools - Cisco DNA Center, vManage

Purpose built for OT use

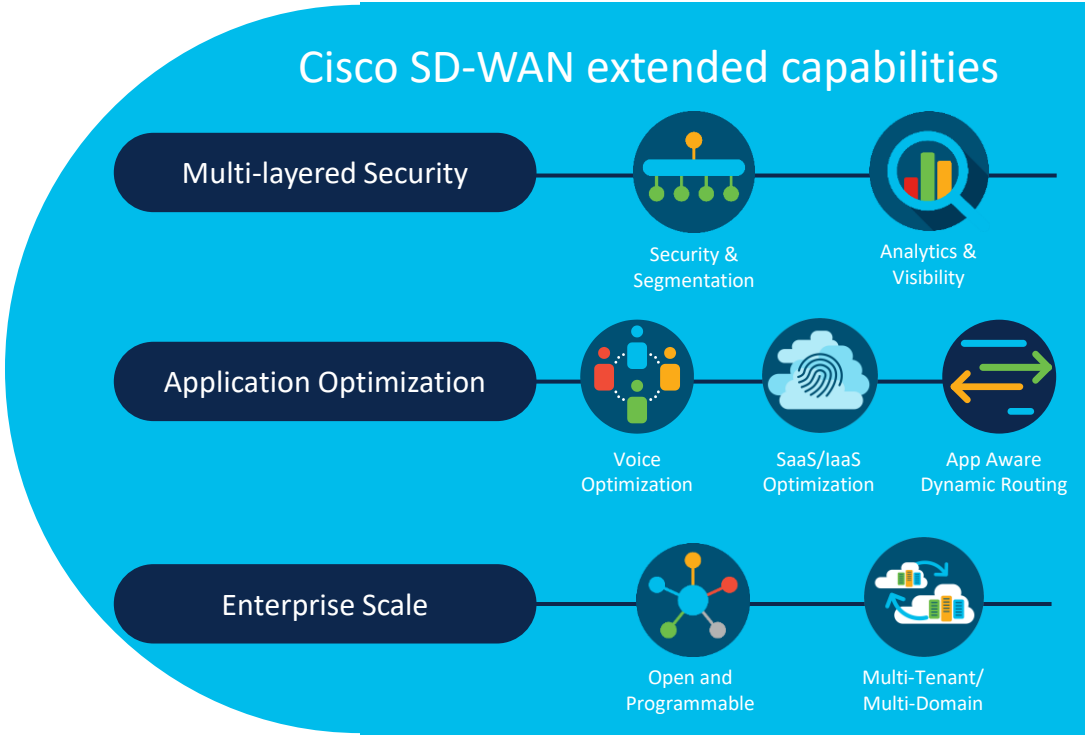
- Built for harsh environments
- Industry use-cases & certifications
- Industrial protocol support
- Operations security & safety
- Built-in edge compute

Cisco IoT

Introducing Cisco SD-WAN

Summary of Basic SD-WAN Capabilities*

- Circuit/Link Load Balancing
- Direct Internet Access
- Centralized Management & Orchestration
- Circuit Cost Savings



*Gartner Critical Capabilities for WAN Edge Infrastructure, December 2018

Benefits of Cisco SD-WAN

Predictable app experience

Support for evolving business application strategy

Cloud OnRamp for IaaS, SaaS and Colocation

Right security, right place

Secure segmentation across entire network stack

Full edge security stack from branch to cloud and colocations

Enterprise grade, simplified

Intent-based networking with multi-domain policy

Proven deployments to over 10,000+ sites

One user interface for security and SD-WAN across branch, cloud, and colocation

SW-Defined Network for SW-Defined Factory

Cisco DNA Center

Cisco DNA Center

Reduce Downtime
Improve network visibility and performance with AI/ML and machine reasoning

Increase Efficiency
Automation and workflows simplify, empower, and streamline network management

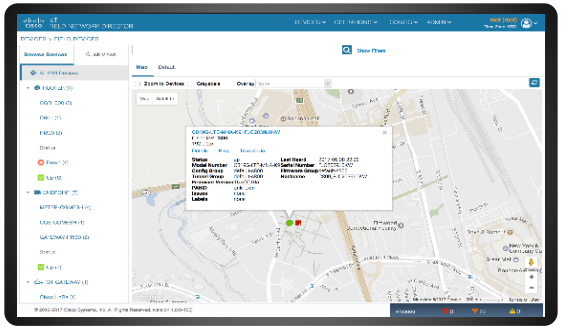
Stay Compliant
Track updates, ensure SW images comply, and remain aware of security updates

Redefine the experience
Platform built on intent-based networking principles and driven by advanced AI and insights

Spend less time managing your operational network

Cisco Field Network Director

One pane of glass



Lifecycle Management

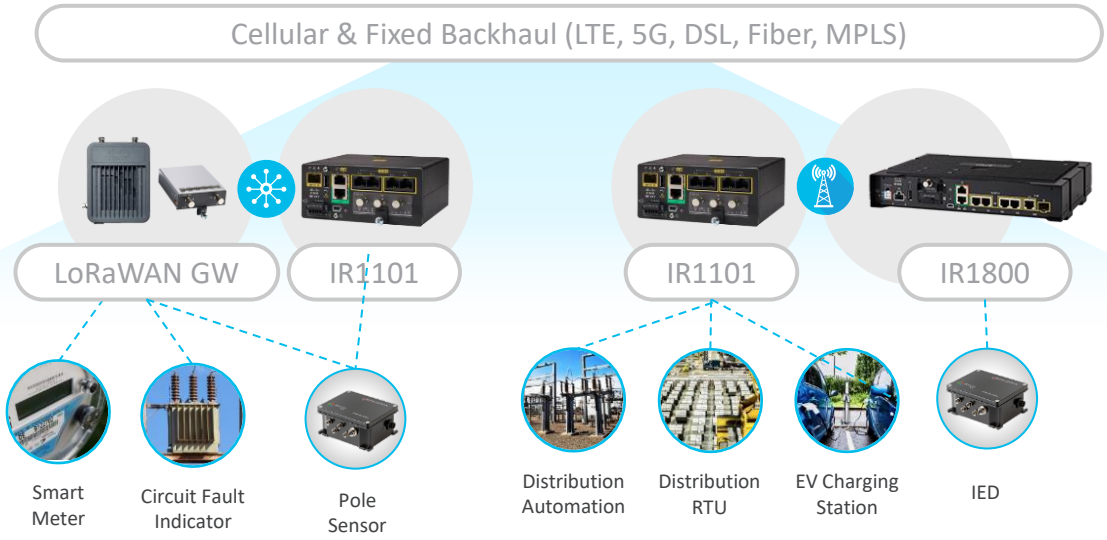
- Automated enrollment and provisioning of gateways and endpoints
- Over-the-air lifecycle management
- Dynamic, customizable dashboard
- Device inventory

Network Optimization

- Configuration management
- Network management for constrained bandwidth
- Network troubleshooting
- User management
- Rich APIs for third party operation application integration

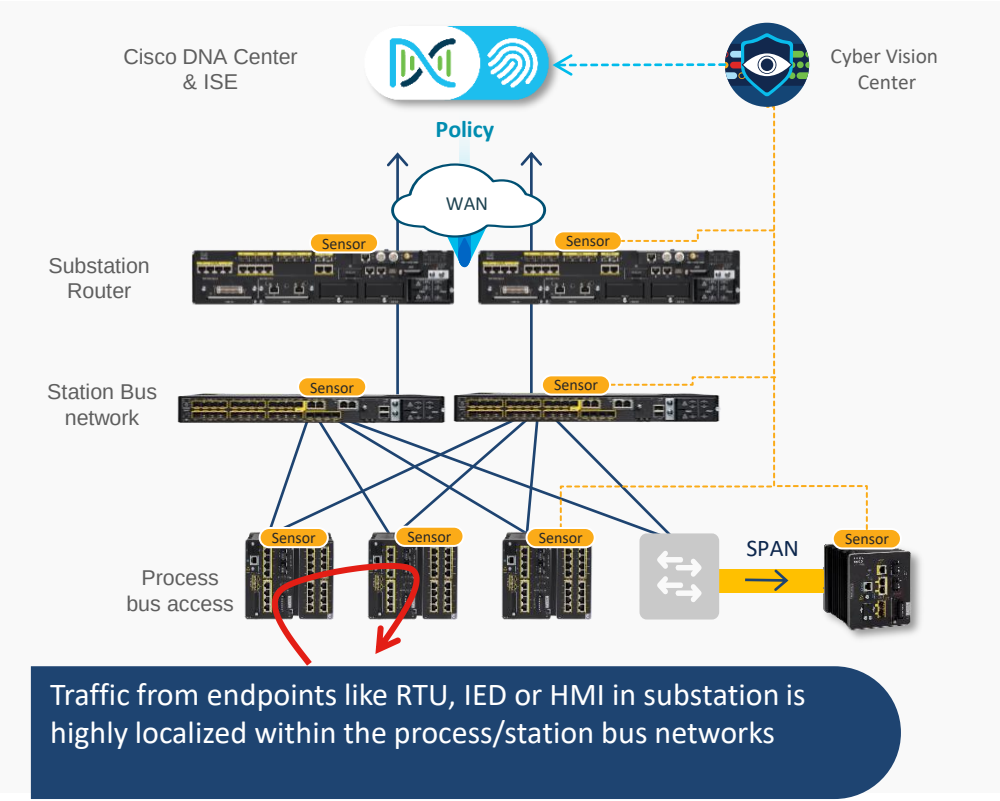
Real-time Monitoring

- Active monitoring and alerts for critical events
- Real-time location tracking of assets and geo fencing
- Rich GIS map overlays



Cisco IoT

DNAC Enables Visualization of Security Policy



1. Discover endpoints and visualize application relationships in **Cyber Vision** to help create TrustSec group-based segmentation policies in **DNAC Access Control Application**
2. Endpoint grouping in Cyber Vision triggers pxGrid updates and results in dynamic assignment of SGTs in **ISE**
3. Visualize group-based network behavior using NetFlow traffic in **DNAC Policy Analytics**
4. Deploy segmentation policy with confidence using **DNAC Day-n templates** once you are comfortable with the observed network behavior

Predictive Maintenance for your industrial network - proactive identify and mitigate connectivity issues

Network Assurance

Before	After
Hours spent fixing network faults	Resolve issues with a single module click

Automatically detect and prioritize issues

AI/ML-driven remediation for quick resolution

Improve network performance

Cisco DNA Center **Assurance**

Constant monitor of network and devices for up-to-date visibility

AI/ML and machine reasoning for root cause analysis, to find anomalies instantly

Correlated insights,with telemetry data to accurately pinpoint root cause

Guided remediation allows for single-click resolution, allowing machine reasoning automation to close the loop

Cisco IoT

DNA Center Network Automation to drive operational efficiency and streamline maintenance

Base Automation

Before	After
Manual device configuration	Simple automated workflows

Workflows to do in seconds what used to take hours / days

Lower cost of network operations

Bridge the IT skill gap and save time

Cisco DNA Center Base **Automation**

Zero-touch provisioning speeds and simplifies adding new devices (PNP, RMA)

Software image management (SWIM) provides consistency for better network performance

Machine reasoning (MR/ML) workflows automate complex tasks into the simple push of a button

Compliance Checks to ensure changes made to the network ar consistent with your standards

Network Compliance

Before → After

Discrepancy between As-Built vs As-Is network	Insights on deviations to ensure compliance

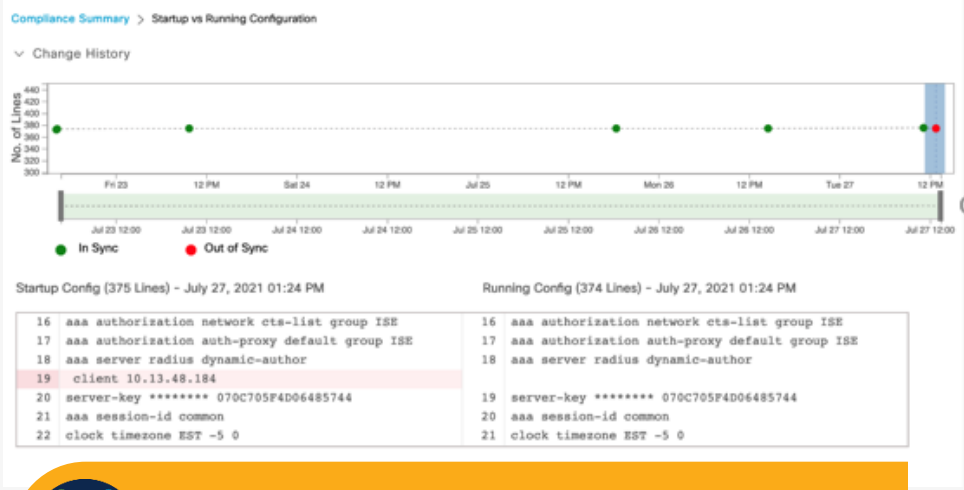
Continuous monitoring for network changes

Audit logging to track who (and what/when) made changes

Cisco Product Security Incident Response Team Alerts

Cisco DNA Center **Compliance**

Configuration Drifts

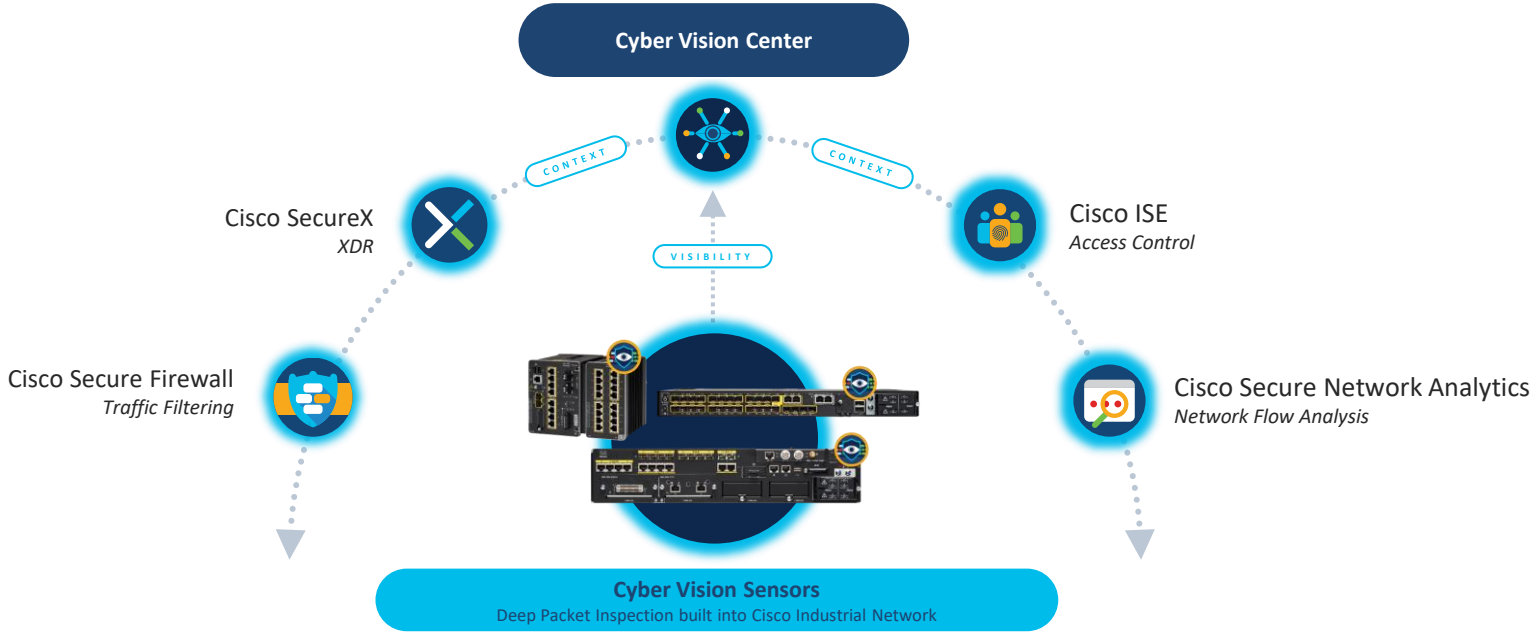


"Golden Image" confirmation for all network devices

Critical Security Advisories – "Psirts"

Industry-leading security built-in, not bolted-on

Operational security features with visibility across the enterprise



Unmatched enterprise-to-edge security • Powered by Talos Threat Intelligence

Cisco IoT

Industry-leading security built-in, not bolted-on

Helping customers achieve NERC CIP Certification

NERC CIP Req.	Area	Technologies applied
CIP-002-5.1a	Critical Cyber Asset Identification	• Cisco Cyber Vision running on IE3400, IE9300 & IR8300 actively and passively identifying connected BES Assets
CIP-003-8	Security Management Controls Access Control	• Cisco's Identity Services Engine (ISE) provides Network Access Control (NAC) for BES Assets, • Cisco network infrastructure implements NAC via IEEE 802.1x • Cisco Duo for dual-factor authentication and • Anyconnect to encrypt remote access traffic
CIP-005-5	Electronic Security Perimeter(s)	• IR8300 Zone-based Firewall and/or • Cisco ISA 3000 Industrial Firewall
CIP-007-6	Systems Security Management	• Cisco's DNA-Center and vManage manage WAN and LAN infrastructure • Firepower Management Center manage firewalls
CIP-008-5	Incident Reporting and Response Plan	• Cyber Vision for anomaly detection for BES traffic • SecureX security orchestration for security events
CIP-010-2	Configuration Change Management and Vulnerability Assessments	• Cisco DNA-Center and vManage report on BES network infrastructure vulnerabilities and compliance • Cisco's Cyber Vision identifies BES asset vulnerabilities configuration changes
CIP-011-2	Information Protection	• Segmentation with Cisco next generation Firewalls, • Micro-segmentation with TrustSec in Cisco network infrastructure • Encrypted communications (e.g. VPN and MacSec), Anyconnect,
CIP-013-1	Supply Chain Management	• Cisco Trustworthy technology against counterfeiting and malicious code • IEC 62443 4-1 (Product development) and 4-2 (Secure Product) certifications

Cyber Vision understands **GRID protocols** you use

IEC 61850

MMS

GOOSE

SV

DNP3

C37.118

IEC 60870-5-104

TASE.2

IEC 60870-5-101

Modbus

DLMS / COSEM

Cisco’s Deep Packet Inspection understands process information
even when using proprietary protocols

The bridge to possible