Renewable Energy—Offshore Wind

Cisco IoT Solution Brief

February 2024

Cisco Validated Design

Cisco Systems, Inc. www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Contents

Cisco Solution for Renewable Energy—Offshore Wind

Providing scalable and secure infrastructure enabling the global accelaration of offshore wind farms.

As we move toward the future, many countries are accelerating the use of renewable energy and investing in grid scale renewable technologies such as:

- Onshore and offshore wind farms
- Solar photovoltaic farms
- Battery storage
- Emerging technologies, such as wave and tidal power

Stakeholders are diverse and range from dedicated renewable energy companies to major oil and gas companies and traditional power utilities.

Reliable and secure connectivity is key for providing for monitoring and control of these offshore and therefore remote assets. Without a reliable and secure communications infrastructure, management and control would be challenging.

From the offshore wind farm operator’s viewpoint, the network needs to be easy to deploy, monitor, upgrade, and troubleshoot. The network design also needs to be standardized to enable easy specification and procurement at the early stages of a project. Avoiding bespoke work and the delivery of different architectures for each project should enable a speedier project delivery phase.

A standardized solution is required that provides the flexibility to meet these needs while facilitating a clear path forward as complexity and scale evolve (for example, larger wind farms, increased number of devices and applications, and increased reliability).

This solution brief provides an overview of the new Cisco validated solution to support offshore wind farms. This solution provides the following key benefits:

- **Flexible deployment options:** Support for simple to advanced solutions that cover various deployment options (scalable for small to large wind farms). A modular design that can adjust to the various sizes of wind farms that are deployed. Provides a flexible platform for the deployment of future services and applications.
- **Rugged and reliable network equipment:** Network equipment designed for harsh offshore environments. The ability for network equipment to operate in space-constrained locations and tough environmental conditions.
- **Simplified provisioning:** Automated onboarding, monitoring, and management of remote networking assets with centralized monitoring and management of multiple wind farm networks.
- **Simplified operations:** Increased operational visibility, minimized outages, and faster remote issue resolution. Compliance of network device configurations (changes from a known baseline are flagged) and firmware and powerful analytics provide deep visibility of the network assets.
- **Multilevel security:** Robust end-to-end security capabilities to protect the infrastructure and associated services, monitor traffic flows, and provide control points for interfacing to third-party networks and equipment. Vulnerability information for discovered assets and asset reporting to aid regulatory compliance (for example, NIS 2 and NERC CIP).

Offshore Wind Farm Connectivity

Generally, offshore wind farms connect to onshore rural locations where access to backhaul technologies is limited. While offshore to onshore connectivity is served by fiber optic cables, the backhaul from the onshore location is more challenging and often relies on service provider network availability for services such as fiber, MPLS, metro ethernet, and so on.

Network Challenges

Multiple Operating Parties

The multiple parties involved within wind farm operations present challenges for network operation and access to required services. The parties can include as the wind farm operator staff, turbine network operation and maintenance (O&M) engineers, substation engineers, and various supplier subcontractors.

These parties all require network access but have different needs for equipment or systems to be accessed.

Environment

Wind farms are challenging environments for communication networks and many locations require environmentally hardened equipment, such as equipment with no fans and extended temperature ranges for operating. However, various locations provide controlled telecom rooms that optionally allow for the use of typical enterprise equipment rather than ruggedized equipment.

Remote and Distributed Locations

Wind farms often are in areas that are underserved by traditional communications networks. A typical operator has multiple wind farms that are distributed regionally or even globally. Each operator has challenges with WAN connectivity to sites and connectivity within sites.

Offshore Locations

Offshore locations provide a unique set of safety challenges for maintenance personnel access. Challenges include weather, salt, spray, and access to offshore assets such as turbines and platforms.

Onshore Locations

While not as challenging as offshore locations, onshore wind farms normally are in remote areas where communication networks are not readily available.

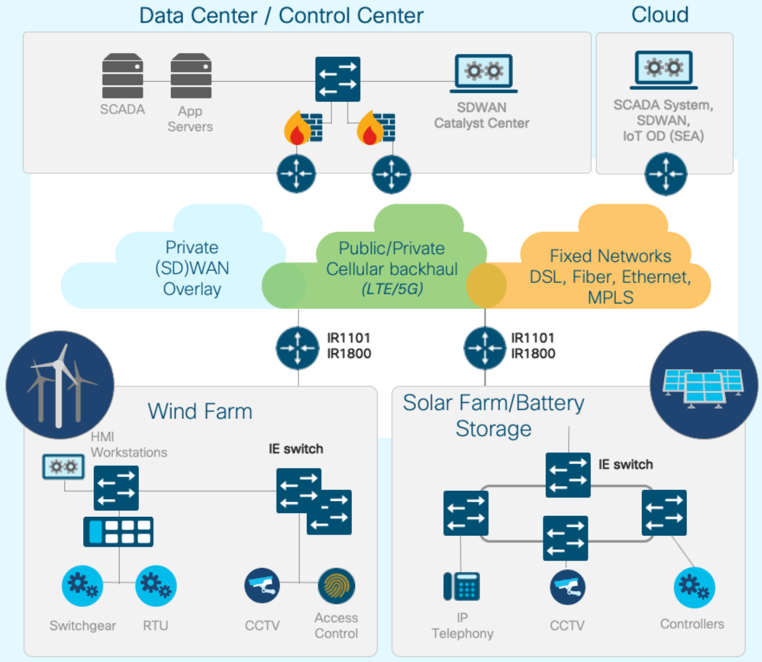
Data Centers

An operator has several data centers that serve the business. These data centers provide many of the services that are required to be accessed from the onshore and offshore wind farm locations.

Resiliency

Remote sites that are used for offshore wind farms need provide highly resilient communications. Most sites require a completely resilient hardware design and architecture to mitigate failures. Typically, this requirement applies to offshore sites where access is difficult. Resiliency is provided through individual hardware resiliency (such as WAN routers, switching network topologies, and power supplies) and network design (use of resiliency features to provide redundant topologies across routers and switches). The goal is to eliminate any single point of failure.

Offshore Wind



Design Considerations

- **Use Cases:**
  - Turbine Control & Monitoring
  - Solar PV Inverter O&M
  - Battery Controller O&M
- **Components:**
  - IR1101 (Cellular, Serial Modules)
  - IR1800 (Wifi6, Unified Threat Defense for IDS)
  - IR8340 for larger sites
  - IR8140 IP67 Outdoor Router
  - Automation & Management
    - Cisco Catalyst Center & SD-WAN
  - Over the top services:
    - Cyber Vision for ICS visibility
    - Secure Remote Access (SEA)
    - Edge Intelligence
  - Cloud Integration

Most offshore wind farm sites participate in the local energy balancing market and are classified as critical power generation sites, which means that the grid can control them in times of over or under demand. These sites may require redundant communications connections, depending upon the business criticality, and may be subject to regulatory cybersecurity conditions (for example, NERC CIP in North America or NIS2 in the European Union).

Due to the remote site locations, redundant communications are usually provided via whatever alternative backhaul technology is available for the site. These technologies could be satellite, fiber, or microwave radio. As an example, microwave radio is a common solution for providing a backup path to primary fiber optic links due to its lower costs of implement.

Remote Access

The following guideline apply to remote access to wind farms. Wind farms require a robust and secure method for providing remote access for employees, suppliers, and contractors.

- Employees, suppliers, and contractors should be able to access a wind farm remotely. Remote access must be provided securely with no separate dedicated “back door” or ad-hoc local connections.
- Users who are authorized to access the network and what applications these users can access should be controlled and managed.
- We recommend the use of bastion hosts or jump servers to restrict users to using only applications that an asset owner authorizes them to access.
- Employees, suppliers, and contractors should use the same method to access assets within onshore and offshore networks.
- External users should be authenticated by using two-factor authentication via the existing enterprise remote access infrastructure to receive access to the bastion hosts only.
- Bastion hosts or remote access servers can provide dedicated and isolated desktop devices with preloaded applications

that can be used to control user access to permitted applications. This approach avoids an employee, supplier, or contractor needing a laptop PC to access critical control networks directly.

- Remote access should provide full logging and auditing capabilities.

Automation

There is a need for a cost-effective operational model for automation, especially one that provides easier deployment, maintenance, troubleshooting, and improved stability and resiliency for wind farm operations.

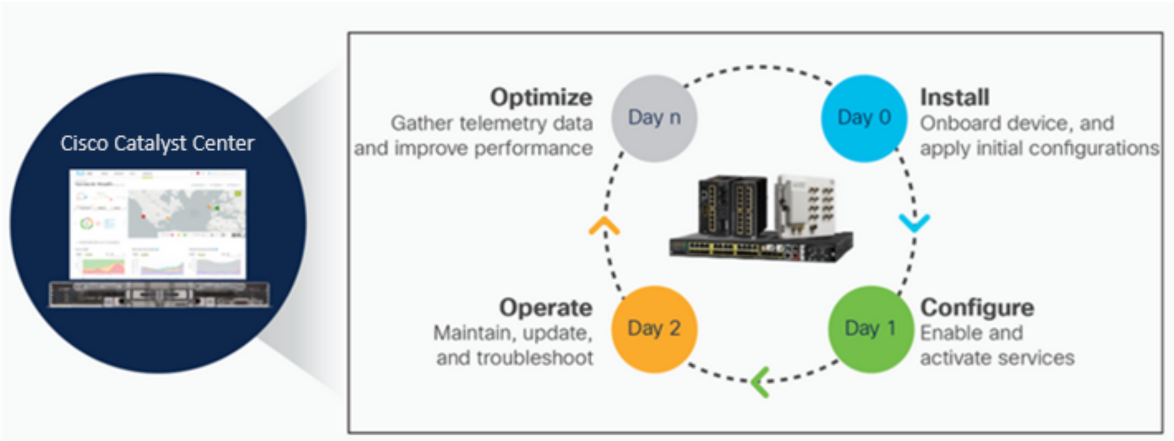
Traditionally, engineering a communications network is a manual task, with equipment configured by using a command line interface (CLI). With the rapid increase of facilities being built and the lack of skilled staff, automation becomes a major consideration for deploying and managing the lifecycle of any underlying WAN and wind farm networks.

The ability to eliminate costly deployment errors (especially errors that affect offshore equipment, which result in a higher cost to remedy) and create repeatable templated system configurations ease the burden of configuring these complex networks.

An offshore industrial ethernet infrastructure often is installed and maintained by personnel with minimal networking background. The results often are network configurations that are consistent when first brought into an operational mode but that drift with time, as a network infrastructure is rarely if ever maintained or improved. Inconsistent configurations, disparate network device software images, and erratic security settings effect system performance and security.

With increased cybersecurity risks, the need to provide end-to-end connectivity while maintaining the highest levels of availability results in a critical need to consistently deploy more sophisticated configurations and maintain them throughout the useful life of a network. Industrial automation systems rely on the consistent, repeatable, and maintainable deployment and operation of sensors, controllers, and other equipment. Why should this approach not apply to the network infrastructure?

Cisco Catalyst Center focuses on deploying and maintaining network infrastructure with automation, offering consistency, reduced effort, and reliance on simplified workflows for both IT and OT personnel. In many ways, Cisco Catalyst Center can be viewed as the “controller” for the network infrastructure.



Cybersecurity

There is a need for a cost-effective operational model for cybersecurity, especially one that provides easier deployment, maintenance, and troubleshooting, and improved stability and resiliency for wind farm operations.

Many wind farms form part of a country’s national critical infrastructure and as such should be protected.

Cybersecurity must be comprehensive and a fully integrated part of the overall network design. Any design should minimize administrative overhead in cybersecurity deployment and operations.

The ability to identify all wind farm assets and their associated vulnerabilities, detect new threats or anomalous behavior on the network, and monitor traffic on an ongoing basis greatly enhances the capability of minimizing the cybersecurity overhead.

Improved security measures are necessary to become compliant with the North American Electric Reliability Corporation Critical Infrastructure Protection requirements (NERC CIP).

The following fundamental principles must be adopted by the network operator to ensure secure systems:

- **Visibility of all devices in wind farm networks**: Traditionally, enterprise devices such as laptops, mobile phones, printers, and scanners are identified by the enterprise management systems when these devices access the network. This visibility can be extended to all devices in a wind farm network.
- **Segmentation and zoning of the network**: Segmentation is a process of bounding the reachability of a device and zoning is defining a layer where all the members in that zone have identical security functions. Designing zones in a network is an organized method for managing device access within a zone and for controlling communication flows across zones. Segmenting devices further reduces the risk of an infection spreading if a device is subjected to malware.
- **Identification and restricted data flow**: All devices in a wind farm network (whether they are OT or IT devices) must be identified, authenticated, and authorized. The wind farm network must enforce a policy when users and Industrial Automation and Control System (IACS) assets connect to the network.
- **Network anomalies**: Any unusual behavior in network activity must be detected and examined to determine if the change is intended or due to a device malfunction. Detecting network anomalies as soon as possible gives the wind farm operations team the ability to remediate abnormalities quickly, which can help reduce downtimes.
- **Malware detection and mitigation**: Unusual behavior by an infected device must be detected immediately, and the security tools should allow remediation actions for an infected device.
- **Traditional firewalls are not typically built for industrial environments**: There is a need for a firewall that can perform deep packet inspection of industrial protocols to identify anomalies in IACS traffic flows.
- **Hardening of the networking assets and infrastructure**. This critical consideration includes implementing key management and control protocols, such as Simple Network Management Protocol (SNMP).
- **Automation and control protocols**: It is important to monitor the IACS protocols for anomalies and abuse.
- **Adhering to security standards**: In the 1990s, the Purdue Reference Model and ISA 95 created a strong emphasis on architecture using segmented levels between various parts of a control system. This approach was further developed in ISA99 and IEC 62443, which brought focus to risk assessment and business processes. A security risk assessment identifies which systems are defined as critical control systems, non-critical control systems, and non-control systems.

Why Cisco for Offshore Wind Farm Networks

Cisco is a global leader in industrial networking and provides a wide range of products to address the offshore renewable energy market. By applying our secure and hardened industrial networking, IoT expertise, and experience working with industry leaders to address challenges in the industry, we have created innovative technology solutions that optimize and secure renewable energy assets. Our goal is to future-proof your investment by providing an evolution path from today's isolated deployments to secure, connected renewable energy deployments that support the energy needs of today and tomorrow.

Since the inception of IP networking, Cisco Validated Designs (CVDs) have been used to validate, architect, and configure industry best practices and technology solutions. CVDs start with solution use cases and architect the flow from edge devices to applications, validating the key Cisco and third-party components along the way. Each aspect of the architecture is thoroughly tested and documented with sample configurations, helping to simplify integration and de-risk implementations through proven solutions.

The goal is to ensure a deployment and a solution that's simple, fast, reliable, secure, and cost effective. Cisco developed renewable energy network solutions to specifically address the networking and security needs of renewable energy asset operators.

Offshore Wind Farm Use Cases

The communications options that are available at a given wind farm site greatly influence the outcomes and capabilities for any use case. The availability of dependable lower latency, high bandwidth connectivity (such as fiber, LTE/5G cellular, or Wi-Fi) allows for more advanced network and data service options, while sites with bandwidth constrains may be limited to simpler use cases such as remote management and monitoring.

Key Use Cases

- **Corporate IT services:** Providing corporate IT access (wired and wireless) to remote sites to enable worker mobility and access to key IT resources. Enabling worker efficiency and the ability to access services such as the corporate intranet, file sharing, and voice and video services.
- **Asset management and monitoring:** Providing access for assets within a remote location for troubleshooting, statistics, or configuration. Usually used for accessing non-operational data.
- **Video surveillance and monitoring:** Monitoring various areas is critical for gaining awareness of activity around a wind farm. With video surveillance cameras, live video streams can be accessed on demand, viewed for immediate response, and stored for future review and assessment. Additional analytics can be deployed on a camera or on localized edge devices, making a camera or edge device a network sensor. Camera use cases include safety such as fire detection, access monitoring, and worker protection.
- **SCADA:** Providing access to and from key operational devices within a remote location. Providing a secure connection to the control center for telemetry and operational data for the turbines and other associated control equipment.

  The types of systems that provide key operational data include:

  - Wind turbine monitoring and control systems
  - Fire detection and alarming systems
  - HVAC systems
  - Power systems protection and control devices
  - Environmental and weather systems
  - Wildlife detection and monitoring systems
  - Lightning detection systems
  - Marine systems (for example, radar and radio)

  These systems usually are key to operating a renewable energy site, providing both monitoring and control capabilities.
- **Secure remote access:** Secure remote access should be provided to allow employees, suppliers, and contractors to access relevant systems for monitoring, troubleshooting, and maintenance. Users should be restricted to access assets based on permissions that are configured with applications such as RDP, SSH, HTTP, HTTPS, and VNC. This approach simplifies troubleshooting devices remotely, with the aim of reducing downtime and onsite support visits.
- **Access control:** Devices providing security related access to remote sites. Includes devices such as keypads, card readers, electronic locks, and sensors that detect open doors or hatches. Reporting data and events to the control center.
- **Meteorological and environmental sensors:** Devices and sensors that are associated with monitoring weather, environmental conditions, and lightning, and specialized devices for specific regional use cases (for example, bird or bat monitors).

- **Radio systems:** Tetra radio is the prevalent offshore solution today for personnel communications. Private LTE is deployed in some offshore projects and provides a more capable data solution. However, 5G networks are starting to appear and provide a platform for several use cases, such as mission critical push-to-talk, service operations vessel connectivity, turbine SCADA network backup, drones for inspection, and support for remote expert workers (using cameras, video glasses, and so on).

Offshore Wind farm Cisco Validated Design

As digital technology is increasingly required to operate remote wind farm locations, equipment must be installed with close attention paid to ease of operations, management, and security. Cisco Validated Designs are simple, scalable, and flexible. They focus on operational processes that are field-friendly and don't require a technical wizard. Our centralized network device management (Cisco Catalyst Center) and strong networking asset operation capabilities eliminate the need for manual asset tracking and inconsistencies in field deployments from one site to another. Integration with operations ensures that field technicians can easily deploy and manage devices without the need for IT support, while IT and OT teams have full visibility and control of the deployed equipment.

Additionally, Cisco provides a wide range of connectivity options, from fiber to cellular or high-speed wireless where hardwired connections are not available.

Cisco has launched a complete validated design for offshore wind farms. This design focusses on an end-to-end architecture for the asset operator's network, including both onshore and offshore locations.

The Cisco Validated Design provides the capability to securely interface with third-party networks such as the turbine SCADA network, export cable system, and the substation protection and control network. Cisco security technologies such as Trustsec working with Cisco Catalyst Center and Cisco Identity Services Engine (ISE) also allow centralized security policies to provide network segmentation.

The Validated Design provides a flexible network to allow additional services to be added as needed while maintaining segregation of traffic. This flexibility includes both wired ethernet switching and Wi-Fi networks, which are available at the offshore substation and turbines. Additionally, Cisco Ultra Reliable Wireless Backhaul radios are used for high bandwidth situations such as service operations vessel connectivity.

The Cisco Validated Design utilizes various Cisco platforms and technologies for automation, configuration, and monitoring, including Cisco Catalyst Center and switch features such as plug and play (PnP).

The Validated Design addresses the WAN handoff interface and new technologies, such as Cisco Catalyst SD-WAN for automating deployment of overlay networks across multiple underlying WAN technologies.

Finally, the Validated Design addresses innovation areas such as solutions for service operation vessels (SOV), providing high bandwidth connectivity for corporate workers and contractors when operating offshore.

The Validated Design is built on the following functional blocks:

- Wind farm operator data center
- Wind farm WAN
- Onshore DMZ
- Onshore substation
- Offshore DMZ
- Offshore substation
- Turbine control network (SCADA)
- Turbine power automation and control network
- Turbine plant IT network (for example, enterprise and plant services)

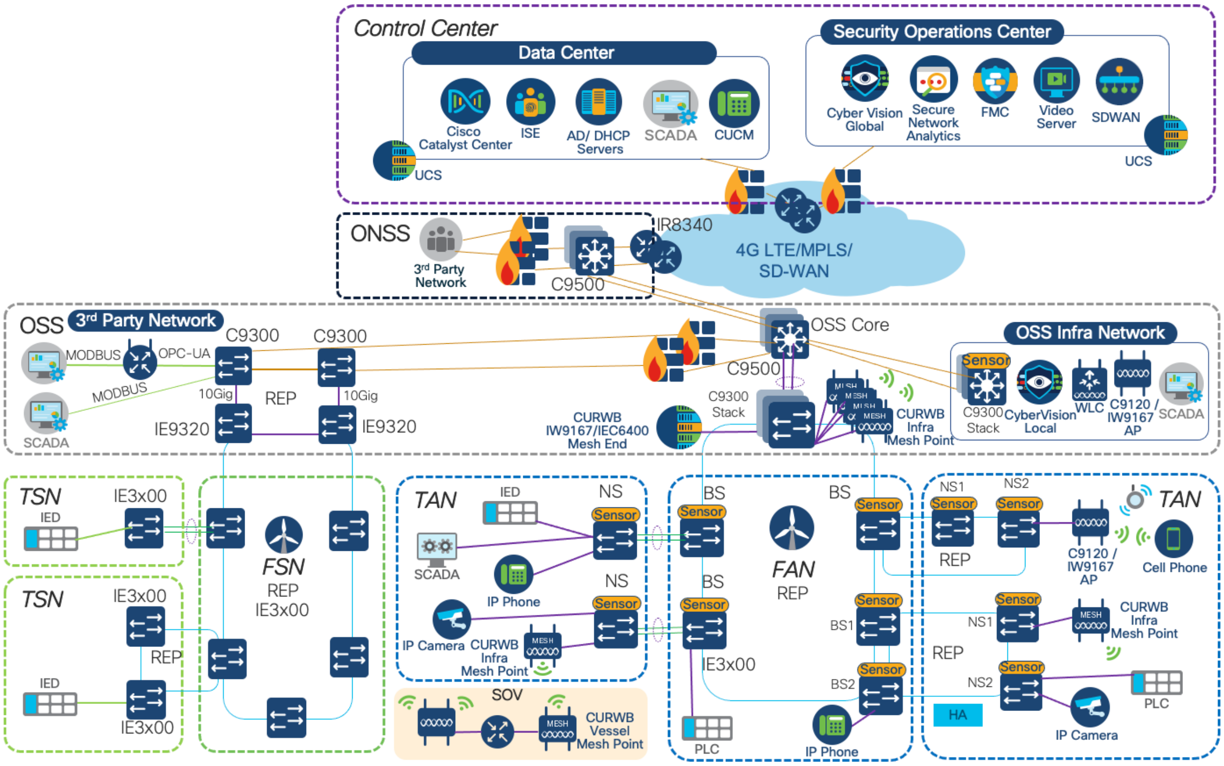
- Offshore service operations vessels (SOV)
- Operations and maintenance buildings (O&M)

The validated design is modular and allows customers or partners to select which modules are applicable to a certain project or deployment or to utilize the entire complete end-to-end validated design.

For the current release, the following functional block is out of the scope of the detailed design. This functional block is covered by the Substation Automation validated design:

- Power automation, control, and metering network:
  - Provided and validated by the power automation and control supplier
  - Offshore and onshore substation equipment and turbine switchgear and IEDs
  - Uses separate fibers (for onshore, offshore, and turbine networks) and a dedicated network based on IEC62439-3 PRP (Parallel Redundancy Protocol) and High-Availability Seamless Redundancy (HSR)

The turbine control and power automation networks typically interface at the onshore or offshore DMZ locations. This approach allows traffic inspection and security rules to control the flow of traffic from these third-party managed systems to the asset operator's network.



The Cisco Validated Design provides several resilient and non-resilient topologies for the turbine network and resilient rings for connecting the turbines to an offshore substation aggregation point.

It is increasingly common to use rings within the turbines themselves, and for the connectivity between turbines (each physical string of turbines is connected via two pairs of fibers in a ring topology). The various turbine rings aggregate at the offshore substation on pairs of aggregation switches. The level of redundancy depends on customer or supplier specifications, but the Cisco Validated Design provides tested solutions for all scenarios (high availability and non-high availability).

Offshore Wind Farm Site Multilevel Security

Wind Farm Security

- Build a dynamic inventory of all devices and their communications patterns
- Segment communications within the onshore and offshore zones and the local DMZ
- Monitor and detect abnormal traffic behaviors
- Contain malware and other attacks
- Integrate operational and enterprise security

Any industrial infrastructure is at a constant cyber and physical security risk. As devices become connected, the attack surface increases. A secure wind farm architecture requires a multilayer approach that includes the physical security of offshore assets, security of network equipment ports, security of application-level traffic, and network segmentation. Our solution integrates all layers of security to keep equipment, applications, and data secure.

Segmentation is the process of isolating certain traffic types by using virtual networks (for example, VLAN and VRF). This approach provides an administrator with additional control for applying security or quality of service to that traffic. These actions often are referred to as macro segmentation.

Micro segmentation provides another layer of segmentation to further isolate equipment on the same virtual network. The micro segmentation capabilities used with port level security ensure that only known devices are allowed on a network and that a specific policy is in place to control which devices and equipment can communicate with each other. In some cases, this control can be down to the protocol level.

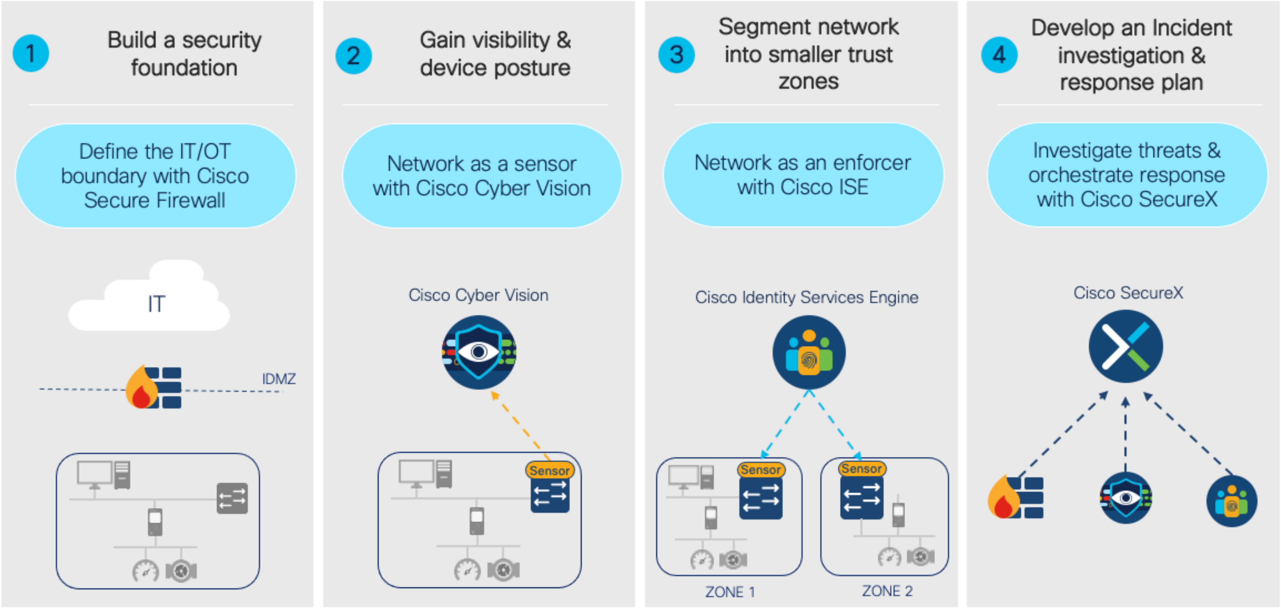
Securing the perimeter ensures that all traffic entering or exiting onshore and offshore networks is controlled and inspected where required.

Validated design security control points include the following:

- DMZ at a data center
    - Normal enterprise security model for incoming WAN connectivity
    - Clustered firewalls for IDS and IPS
- DMZ at onshore substation
    - Redundant firewalls for IDS and IPS
    - Secure local perimeter for third-party network connections
    - Monitoring traffic flows for known threats
    - Blocking undesirable traffic
- DMZ at offshore substation
    - Redundant firewalls for IDS and IPS
    - Secure perimeter for third-party network connections
    - Monitoring traffic flows for known threats
    - NAT for third-party networks
    - Blocking undesirable traffic

The security design is built as shown in the following figure. Each step adds value and provides a clear benefit to the overall security posture of a wind farm.

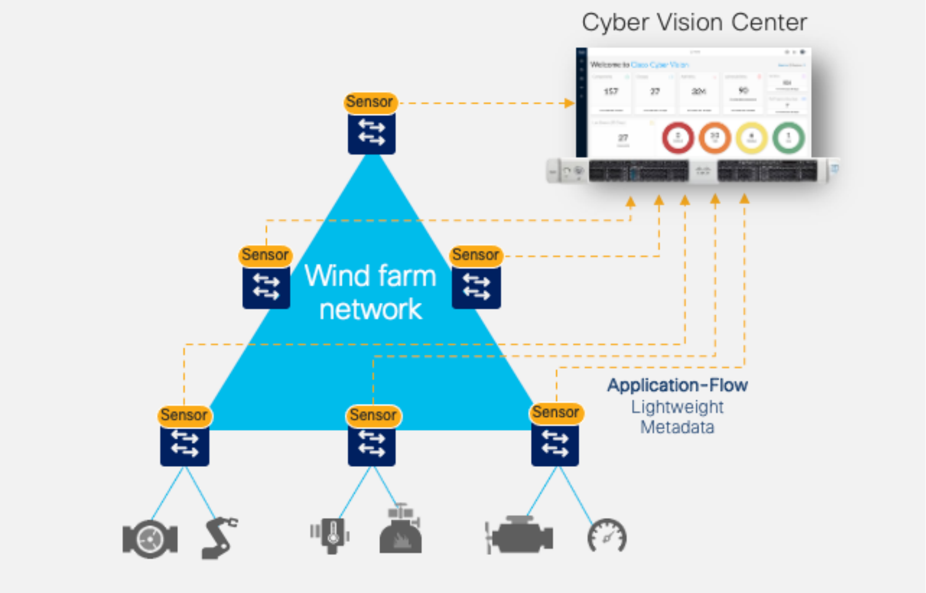
Industrial Security Guidelines


1
Build a security foundation
Define the IT/OT boundary with Cisco Secure Firewall
IT
IDMZ
2
Gain visibility & device posture
Network as a sensor with Cisco Cyber Vision
Cisco Cyber Vision
Sensor
3
Segment network into smaller trust zones
Network as an enforcer with Cisco ISE
Cisco Identity Services Engine
Sensor
Sensor
ZONE 1
ZONE 2
4
Develop an Incident investigation & response plan
Investigate threats & orchestrate response with Cisco SecureX
Cisco SecureX

Cisco Catalyst Center, interfacing with Cisco Cyber Vision, and Cisco ISE can help secure your operations:

- Establish a security profile to manage industrial networks
- Create authentication and authorization policies in ISE
- Visualize connected industrial assets in Cisco Catalyst Center as discovered and profiled by Cyber Vision and grouped in ISE
- Monitor communications patterns between asset groups using NetFlow traffic and help define and validate access policies
- Create and manage cybersecurity segmentation policy (Trustsec and Scalable Group Tags (SGTs)) for a wind farm network
- Deploy policies with confidence and segment the network to restrict unnecessary access
- Allow use of other Cisco security applications, such as Umbrella, Secure Network Analytics (Stealthwatch), and SecureX for further enterprise security integrations

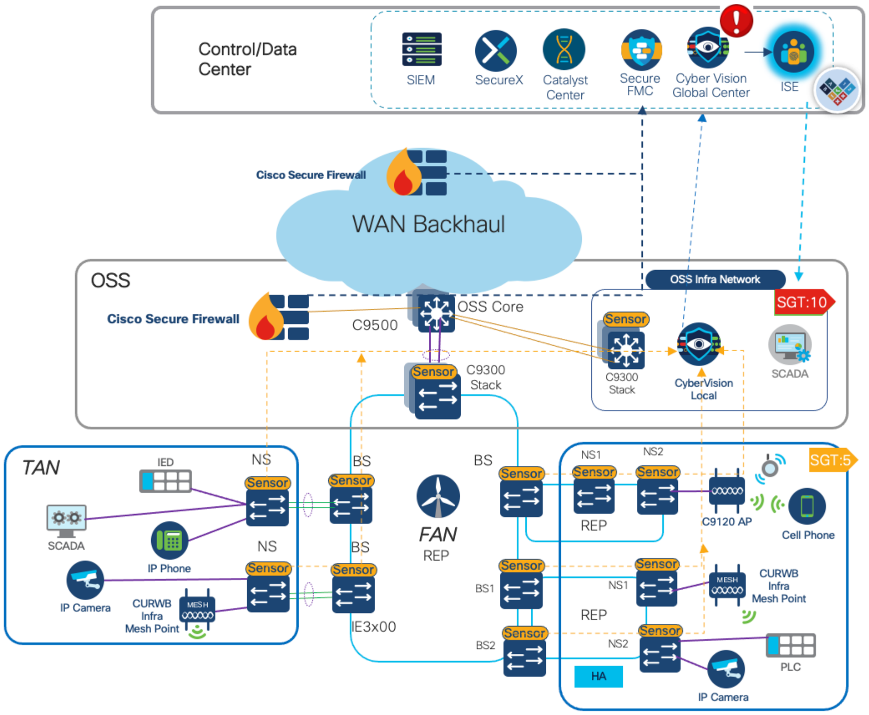
In industrial environments, network-based monitoring capabilities typically are deployed using switched port analyzer (SPAN) ports instead of in-line network taps that could create a communication point of failure. Cisco Cyber Vision provides a unique approach that uses sensors that are embedded into network equipment. Cyber Vision sensors are embedded in Cisco switches and routers to analyze packets that flow through the industrial infrastructure. Using a combination of passive and active discovery techniques, a sensor leverages advanced knowledge of industrial protocols to decode and analyze packet payloads through deep packet inspection (DPI). This approach lets Cyber Vision profile each endpoint, detail endpoint interactions with other endpoints and resources, and build an asset inventory.



Benefits of Cyber Vision include scalable real-time cyber security protection from external and internal threats, and include the following:

- **For network operations:** Ability to consistently apply security policies, deploy security updates, and protect against unwanted devices or applications on the network. Ongoing monitoring and analysis of network with automated anomalous network traffic detection and alerts and the ability to instantly quarantine suspect devices or applications.
- **For field operations:** Visibility to offshore networks, quickly deploy equipment without having to understand complex security deployments. Know that critical applications are available and operational at offshore locations.

The following diagram illustrates the use of Cyber Vision in a validated network architecture.



1. Implement IDMZ and basic segmentation
2. Cyber Vision discovers industrial assets and communications and groups it into Zones.
3. ISE implemented for visibility and Cyber Vision context is shared with ISE.
4. Components are dynamically classified in SGTs via group assignment directly from CyberVision
5. Visualize traffic activity between SGT in Catalyst Center policy analytics
6. Deploy segmentation with confidence once you are comfortable with the observed network behavior
7. Cyber Vision or other analytics tools raise alarms endpoint behavior anomalies and threat detection.
8. Investigate in SecureX and SOC tools
9. Users can trigger quarantine of offending asset.

Conclusion

The demands for robust and connected solutions with a network infrastructure that is simple to manage and operate are essential to support renewable energy networks at scale. The Cisco wind farm solution provides the capability to address different deployment options while maintaining a single provisoning and management application with built in cycbersecurity.

Cisco Offshore Wind Farm Network Benefits

- Pre-validated, proven multiservice network for your present and future goals
- Ruggedized network for robust and effective movement of data
- Automated service segmentation to simplify security policies
- Centralized security policy control
- Plug-and-play device deployment for simplicity and efficiency
- Automated uniform policy deployment for one redundant and resilient network
- Flexible network topologies and backhaul options for future services and growth opportunities

Resources

- Cisco Utility & Renewable Energy Validated Designs
- Cisco Industrial Routers and Gateways
- Cisco Industrial Switches
- Cisco Cyber Vision
- Cisco Catalyst Center
- Cisco Identity Services Engine