PNDC and Cisco Security Demonstration Facility

Why is Security Critical for Power Utilities?

Why is Security Critical for Utilities?

The evolving power of the utility landscape

After what seemed like decades of stability and predictability, power utilities have entered a new era of change and uncertainty. Security threats are growing, regulations are tightening, and new technologies—from electric vehicles to microgrids—are disrupting longstanding business models. Meanwhile, consumers are demanding more from their energy supplier, from flexible pricing to sustainable energy options. These trends have changed the game for utilities, forcing them to either evolve or face diminishing growth and profitability.

External and internal factors are changing the nature of the distribution network. The growing adoption of solar, wind, and other renewables has challenged power utilities to adapt by integrating these distributed energy resources into the grid. This is not a simple process, given the challenges of implementing bi-directional power flows. Power utilities are also moving to add more intelligence into their networks, so the infrastructure can be used more efficiently, and the effect of faults mitigated more quickly. Active network management can deliver operational improvements but also increases the reliance on communications compared with traditional approaches.

Recent security incidents—both cyber and physical—have sent shock waves through the industry, resulting in new regulations to avert crippling attacks on critical energy infrastructure. Yet most power utilities have a long way to go to protect their grids. Isolating the network is no longer an option. The reality is that power utilities must be connected to increase grid efficiencies, improve resilience and—ultimately—deliver the next generation of services to an increasingly digitised and mobile customer base.

Digitalisation and connectivity are the core of future smart grid technology. They extend its capability to effectively balancing demand and supply in real time, offer an efficient platform for power networks with better reliability and enable secure delivery and cost-effective service to consumers.

To thrive in this new era, power utilities will need to invest in more efficient, automated, and resilient energy grids. However, the industry's infamous ageing infrastructure – together with a shortage of younger workers with new, relevant skills joining the industry – complicates the task. Strategy-minded power utilities are increasingly planning for a future based on IT and smart grid applications that require advanced telecommunications systems. IP-based, packet-switched networks will form the backbone of these new systems, providing system interoperability and enabling a spectrum of new applications that improve grid security, control, and automation.

Perhaps most promising - and most exciting of all-connected-grid technologies will offer power utilities a broad platform for innovation. This will help unlock the power of the latest iterations of the Internet of Things (IoT), artificial intelligence, and predictive analytics. With utilities estimated to have more intelligent devices in operation than anywhere else, the potential for capitalising on this built-in IoT network—and the terabytes of data it holds—is enormous.

If utilities are to comply with new regulatory requirements, cope with an ageing infrastructure, improve workforce efficiency, and address new customer expectations, they must place digital transformation at the top of their business agenda.

There are in fact, many priorities for today's power utilities, including the transition from DNO to DSO, complying with new regulations, accommodating rising consumer empowerment and integrating new energy sources and consumption models.

In addition, with the growing need to for digital connectivity across the sector, cyber security, data integrity and confidentiality will be particularly important.

What is Operational Security?

Alongside the benefits of this digital connectivity, we must also consider the hazards of connecting this critical infrastructure to the network. News and social media outlets regularly report on how the networks of well-known organisations and governments have been compromised by hackers. With power utilities critical infrastructure now connected to the network, it is possible that it too could be vulnerable to hackers.

What was previously a point-to-point serial connection – with a known (and presumably trusted) source and destination – can now, without proper access restrictions, become an attack vector into the industrial network and, more importantly, critical national infrastructure (CNI). Instead of simply managing physical access to either endpoint of the point-to-point serial connection, we must now protect every ingress point into the network from a much larger pool of attackers – possibly all endpoints connected to the respective network – public or private, local or remote.

There are three high level rules of operational security and how to manage risks:

1. **Know your assets**
2. **The threats to those assets**
3. **You don't comply with rules one and two, the enemy wins**

Meanwhile, the four major steps of risk management are as follows:

- **Risk identification –** identify all the tangible and intangible assets that your organisation cares about.
  This includes the creation of a risk register and mapping out risk scenarios during the identification.
- **Risk assessment –** assess the threats and threat actors for the vulnerabilities across the identified assets.
  There are several assessment methodologies that are typically used (NIST, ISO, COBIT and OCTAVE to name a few); this step also updates the Risk Register.
- **Response (or risk treatment)–** the business is now able to define which risks need urgent treatment and apply the appropriate controls, monitoring and reporting.
- **Monitoring and reporting –** Keep re-assessing whether the controls are performing the way they should and whether any new threats have emerged.

Risk Management

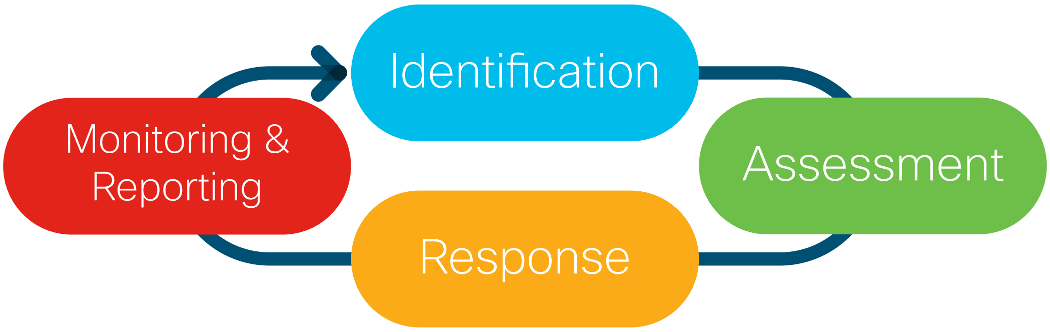


Figure 1 – Risk Management Chart

What is Operational Security? (Part 2)

As we consider each one of the possible numerous attack vectors and associated responses, we must ensure that the critical infrastructure remains operational.

The multi-faceted approach that we will use to ensure high reliability and resiliency of the network includes:

- **Protecting -** putting best practice safeguards around the critical infrastructure – including physical, logical, and policy safeguards – to significantly restrict and defend access to the network from nefarious users.
- **Detecting -** using logging, accounting, and context-based traffic analysis to understand what is accessing your network – and from where – at all times.
- **Deterring -** managing the risk versus reward of the attack appropriately can sufficiently discourage the attacker from attacking the infrastructure.
- **Preventing -** targeted logical or physical controls ensure that any attempts to attack the infrastructure are mitigated and will fail.
- **Limiting -** if an attack does happen, the scope and length of the attack on physical and logical assets is mitigated, as well as any potential damage to reputation.
- **Recovering -** following an attack on the infrastructure, ensure that the business can return to normal operation quickly and with minimal or no long term affects.

Operational Security Best Practice Methodology

The Enterprise Security Architecture (ESA) model outlines this best practice approach, which is equally applicable to the operational domain.

The methodology is based on three primary pillars: **what, why and how.**

1. **What:** identifies the core assets that need protection (such as branding, IP, strategic partnerships, etc.). This can be a combination of both tangible and intangible items.
2. **Why:** details the reasons why we need to protect those assets.
3. **How:** defines the controls that are used, these can be products, services and solutions that minimise the risks identified in the "why" phase.

The Enterprise Security Architecture Model

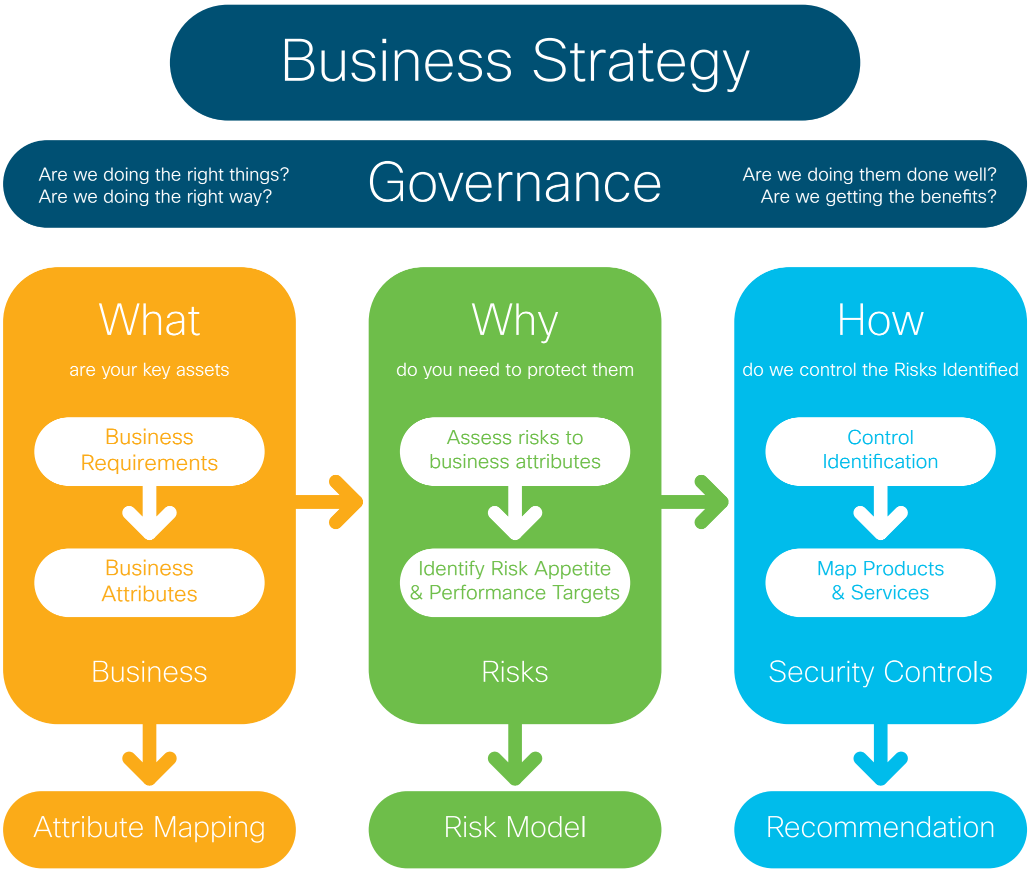

Business Strategy
Are we doing the right things?
Are we doing the right way?
Governance
Are we doing them done well?
Are we getting the benefits?
What
are your key assets
Business Requirements
Business Attributes
Business
Why
do you need to protect them
Assess risks to business attributes
Identify Risk Appetite & Performance Targets
Risks
How
do we control the Risks Identified
Control Identification
Map Products & Services
Security Controls
Attribute Mapping
Risk Model
Recommendation

Figure 2 - Enterprise Security Architecture Model

As part of the **how** phase - and in order to enable the multifaced approach to security - we need to implement a set of security best practices across the operational network.

These are as follows:

Asset Inventory

One of the first steps in risk assessment is understanding and validating the installed equipment in remote locations, such as low voltage substations.

This is a critical element to securing the organisation, especially as the use of Ethernet/IP sensors means more and more locations become connected.

The asset inventory needs to extend to all devices including communications equipment, SCADA RTUs and IED and smart sensors.

This should also be performed periodically and allows vulnerabilities to be cross-referenced against the assets and the specific protocols in use.

Any devices on the network that the organisation is not aware of are points of vulnerability and it is hard to protect what can't be seen.

Once all devices are identified and known, it becomes easy to detect and remediate threats that may bypass existing controls.

The Enterprise Security Architecture Model (Part 2)

Identity and trust

Today, many remote substations rely on physical security to stop unauthorised access. This is often in the form of a padlock and master key.

This needs to change, so that physical security and cyber security are combined. This ensures identity of people and devices in the substation are understood and authorised against their activities. The identification of traditional RTUs, PLC and IED has often been a challenge due to these devices not being able to use techniques such as 802.1x or x509 certificates.

Whilst this is improving, it is still important to identify all devices, including older but essential legacy devices, to ensure they do not compromise the security of the overall utility.

All new substation devices should ideally now have a strong, non-reputable identification, with each device announcing itself to the network using authentication that can be verified by some type of authority to establish trust.

The identification of each device is also critical in determining which other devices it can and should communicate with.

Fine-grained access policies with real-time enforcement

Fine-grained network access control policies will determine what devices are allowed to do on the network. The diversity in IoT device types, locations and business functions, demands more policy variety and granular enforcement rules than we typically see across the IT domain in other sectors.

As already highlighted, device identity, posture and behaviour will determine how these network access policies are enforced. For example, untrusted devices, or those exhibiting anomalous behaviour, may be denied network access or quarantined to a particular network segment.

Dynamic traffic shaping and network micro segmentation

The goal for security in the substation is for identity, device type, transport protocols and data/application sensitivity to define network segmentation policies. Today, we typically base segmentation on techniques such as VLANs.

However, this technique cannot cope well with the dynamic changes required. New software-defined networking (SDN) techniques such as scalable group tagging will be used to enforce segmentation across layer two and three networks based on identity and posture.

The Enterprise Security Architecture Model (Part 3)

Visibility and analysis

IoT will fuel the existing need for big data security analytics, as security analysts investigate suspicious IoT traffic and IoT-based malware attacks.

Once the initial levels of segmentation have been implemented for known IoT devices and users, adding improved methods of visibility enables identification of undocumented devices on the network as well as helping companies better understand their networks. This enables operators to see changes that could indicate potentially dangerous behaviour to and from IoT devices. It is key that the following functions are performed:

- **Monitor infrastructure communications flows -** using the information to better pinpoint nuisances in the network and identifies and alerts on abnormal device traffic flows.
- **Normal IoT network behaviours -** this creates a baseline for operations and known devices connected to the network and generates alerts when abnormal activities occur.
- **Threat intelligence–**provides knowledge of existing malware and communication vectors and learned knowledge of emerging behavioural threats.
- **Intrusion prevention–**gives IoT visibility with deep packet inspection; blocks attacks, exploitation, and intelligence gathering.
- **DNS based security–**identifies Internet communications from every device on the network.
  This is based on name resolution and can block malicious domains. It can also break command and control call-backs.

Power utilities should also expect to start sharing threat intelligence data with other utilities, industry ISACs, government agencies, and security vendors.

Secure remote access

To maintain the expensive and sophisticated operational infrastructure, utilities often rely on vendors for debugging and maintenance. This requires them to have remote access into the substation. Secure remote access replaces the legacy modems and other connectivity methods vendors used in the past, eliminating the back doors to their digitally connected network.

- **Secure remote access VPNs–**provides secure encrypted access for remote operators, vendors, and providers based on roles and policies.
- **Client and network security–**inspects files for malware and viruses, quickly quarantining and removing threats before they can spread and contaminate vulnerable IoT systems.

Network encryption

While utility organisations already use encryption on some wide area networks, it's likely that IoT will drive more granular implementation. SDN network segmentation may also trigger point-to-point/point-to-multi-point encryption based upon network segments, protocols, or network flows. As networking equipment and digital certificates come together, point-to-point encryption will be based on SDN/PKI amalgamation.

The Enterprise Security Architecture Model (Part 4)

Greater network intelligence, data sharing and automated remediation

Rather than just adding security components that work in isolation, security solutions need to be internetworked so that they work together to produce superior intelligence, allowing rapid and often proactive response.

IoT-enabled security solutions will generate vast amounts of data, making it impossible for human beings to keep up with threat intelligence and alerts, or adjust security controls in lockstep with real-time requirements. Therefore, IoT-enabled security solutions must support the communication and consumption of machine-to-machine intelligence for immediate, automated security control, without human intervention.

When security events are detected, the entire security network needs to consume the alert and take the appropriate action. For example, cameras can focus on the appropriate areas; doors in the affected areas can be locked; and access to critical systems can be disabled. Meanwhile, alerts sent to security personnel can initiate the appropriate human response.

As well as demonstrating best practice, these security principles are now being mandated by government directives. A key change in UK policy has been the introduction of the Network and Information Systems Regulations 2018 (the NIS Regulations 2018).

This is the implementation of the EU NIS Directive in the UK, effective from 10 May 2018. This will help ensure UK operators in electricity, transport, water, energy, transport, health and digital infrastructure are equipped to deal with the increasing number of cyber threats.

To help organisations comply with the NIS Regulations 2018, the National Cyber Security Centre (NCSC) has produced a set of guidelines, which list four major objectives:

Objective A. managing security risk

Objective B: protecting against cyber attack

Objective C: detecting cyber security events

Objective D: minimising the impact of cyber security incidents

The security best practices detailed in this document are critical to aligning with these guidelines and achieving NIS compliance.

PNDC and Cisco Operational Security Test Bed

As part of a long-term partnership, Cisco has designed and installed a state-of-the-art communication test bed at the Power Networks Demonstration Centre (PNDC), to represent all aspects of communications that might be found in a power utilities network. These include sensor networks, different size substations and a high speed MPLS core running over a DWDM Optical network.

Across all these various communication technologies, Cisco has embedded cyber security into the design and implementation, to address the concerns highlighted in the previous section.

High level network components:

- Data centre with application and management services.
- Core DWDM optical network.
- High speed MPLS running teleprotection.
- Five substations, ranging in size from primary to secondary, including resilient digital substation local area networks and wireless infrastructure.
- Field area network communications.
- Low powered wide area network (LPWAN) technologies for sensors.

In addition to communication components, operational assets such as RTUs, protection relays and IED have been deployed for testing different security scenarios and analysing the impact of modern security techniques on traditional operational devices.

This results in an industrial cyber range that allows utilities to validate security architectures and assess current compliance. The facility can also launch cyber-attacks to see how the systems respond, e.g. rapid threat containment for quarantining non-critical assets under attack.

The following is a sample of the capability of the test environment:

- Validate current and future security architecture.
- Assess impact of security technologies on traditional operational equipment.
- Test new operational devices for security compliance.
- Test new operational devices for integration into modern communication networks.
- Develop mitigation techniques for legacy operational estate.
- Assess current operating procedures against security principles and compliance.
- Penetration testing in safe environments.
- Identify vulnerabilities and assess impact or attacks on the operation network.
- Test operational procedures and remediation against typical attacks.

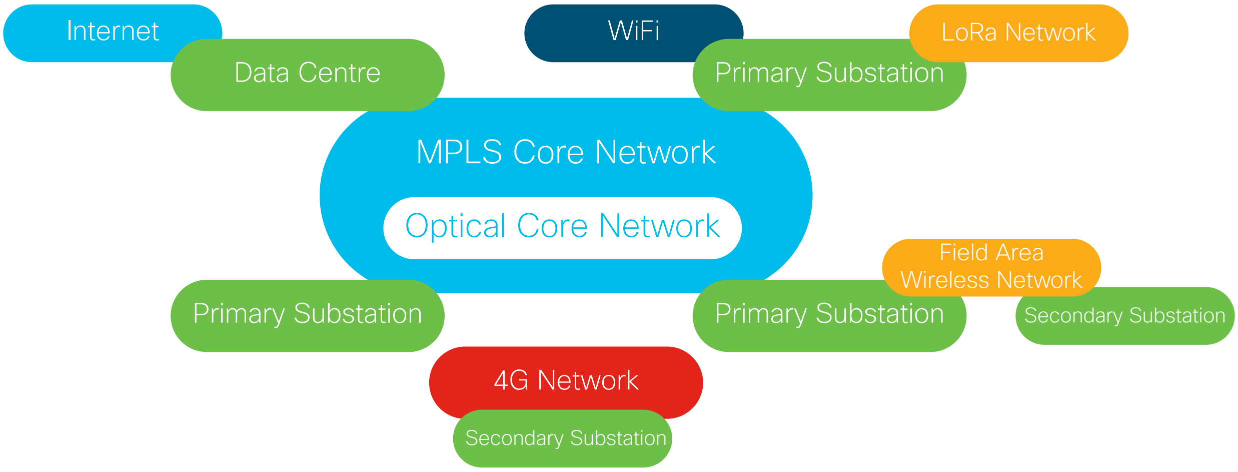


Figure 3 - High level architecture of the installed communication platform in PNDC

The Power Networks Demonstration Centre

The Power Networks Demonstration Centre (PNDC) is a unique world-class facility that is already playing a leading role in the transition towards a “smart” grid and the acceleration of low carbon technologies.

The PNDC is a research, development, and demonstration centre for emerging technologies with a view to reaching commercial deployment. It offers a realistic and controllable testing environment that helps de-risk potential solutions before connection to the grid. As part of the University of Strathclyde, the centre was founded through collaboration between both public and industrial partners. As a leading international technological university, Strathclyde’s research capabilities and long-standing industry partnerships are helping to develop the next generation of electrical power systems technologies.

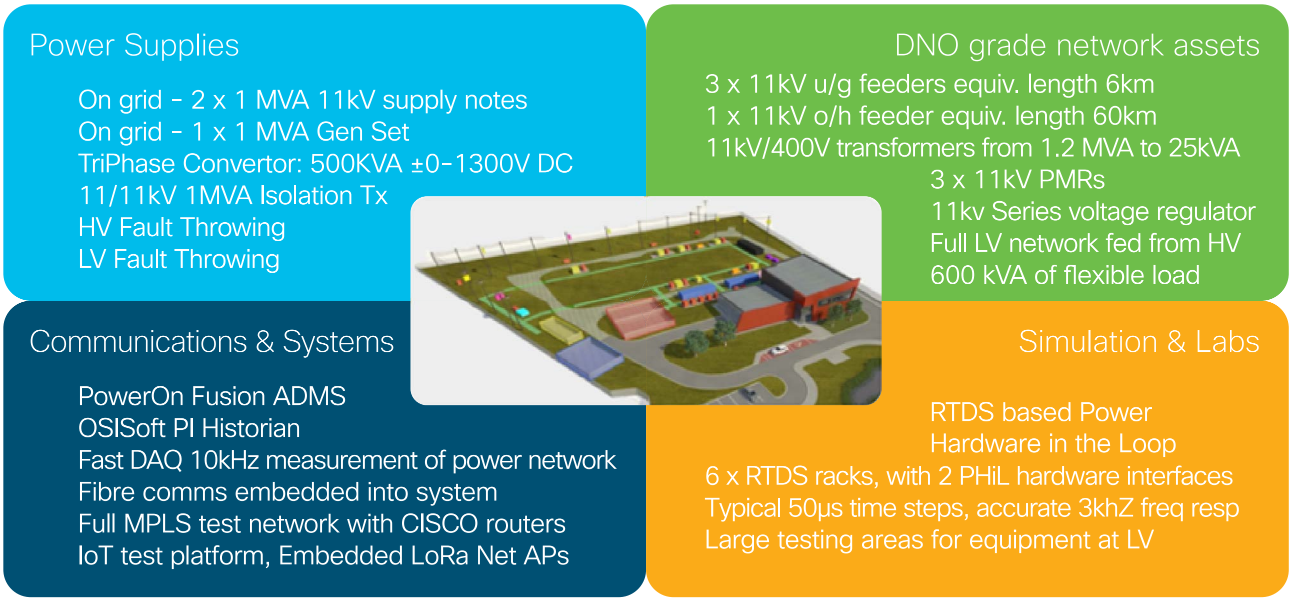
The PNDC works closely with its industrial partners, including power utilities and global technology companies, delivering industry leading research to accelerate the adoption of innovation across energy networks. Our open-access facility contains an 11kV distribution network, which offers a realistic electrical network layout and characteristics.

To provide a safe and controllable testing environment, the facility can be disconnected from the local grid, effectively operating as an islanded energy system. In order to accelerate the transformation towards a smart grid system, a next-generation communications platform has been introduced and installed.

This will be used to integrate the electrical grid equipment with the digital communication networks while providing a framework for designing and implementing comprehensive management and security solutions across the grid. Furthermore, the platform will be used to enhance the network connectivity of the power utility, offer reliable networking across a variety of distributed devices and create cross compatibility between different Smart Grid applications.

The architecture is not limited to any vendor, is flexible and can be reconfigured based on any specific requirements. Moreover, the current testbed will open the door to testing and validating any scenario. It will enable the manufacturers and the DNOs to test any new functionality prior to any commercial deployment.

For more information please visit the PNDC website: www.pndc.co.uk



Power Supplies

On grid - 2 x 1 MVA 11kV supply notes
On grid - 1 x 1 MVA Gen Set
TriPhase Convertor: 500KVA ±0-1300V DC
11/11kV 1MVA Isolation Tx
HV Fault Throwing
LV Fault Throwing

DNO grade network assets

3 x 11kV u/g feeders equiv. length 6km
1 x 11kV o/h feeder equiv. length 60km
11kV/400V transformers from 1.2 MVA to 25kVA
3 x 11kV PMRs
11kv Series voltage regulator
Full LV network fed from HV
600 kVA of flexible load

Communications & Systems

PowerOn Fusion ADMS
OSISoft PI Historian
Fast DAQ 10kHz measurement of power network
Fibre comms embedded into system
Full MPLS test network with CISCO routers
IoT test platform, Embedded LoRa Net APs

Simulation & Labs

RTDS based Power
Hardware in the Loop
6 x RTDS racks, with 2 PHiL hardware interfaces
Typical 50μs time steps, accurate 3khZ freq resp
Large testing areas for equipment at LV

Figure 3 - High level architecture of the installed communication platform in PNDC

Cisco's Security Capabilities

Our utility networking solutions form a unified portfolio of solutions that help utilities modernise, reduce risk and innovate.

Unrivalled security expertise

Cisco is the clear industry leader in network security, with the largest non-governmental security intelligence organisation in the world. No other solution provider can match Cisco's technology firsts, the breadth and depth of its product portfolio, and the continuing commitment to innovation.

Cisco takes an integrated approach to security, intelligently connecting each part of the utility value chain—and every network asset—to create a unified, centrally managed whole. And Cisco keeps innovating, pushing the envelope of what's possible in the field of physical and cyber security integrating functionality such as visibility, malware detection, segmentation, rapid threat containment and retrospection into utility networks.

The new Cisco IOS® NetFlow and Stealthwatch® solutions, for example, are setting new standards for anomaly detection and risk reduction.

Threat Intelligence

Cisco Talos Intelligence Group is one of the largest commercial threat intelligence teams in the world, comprised of world-class researchers, analysts and engineers. These teams are supported by unrivalled telemetry and sophisticated systems to create accurate, rapid and actionable threat intelligence for Cisco customers, products and services.

Talos defends Cisco customers against known and emerging threats, discovers new vulnerabilities in common software, and interdicts threats in the wild before they can further harm the internet at large. Talos maintains the official rule sets of Snort.org, ClamAV, and SpamCop, in addition to releasing many open-source research and analysis tools.

Comprehensive grid management capabilities

Cisco is breaking new ground in distributed control and real-time management of energy grids. Our Evolved Programmable Network Manager for example, provides simplified, converged, end-to-end lifecycle management for carrier-grade networks of all sizes.

Security Management is a key focus, with its effectiveness maximised through the adoption of a fully integrated end-to-end operational security architecture.

Setting the pace in IoT

As digital utilities connect to larger numbers of distributed assets, data volumes are exploding and networks are becoming overloaded. Cisco leads in technologies that intelligently shift data processing and analytics to the network edge, improving performance and decision-making.

Cisco's IOx and Fog capabilities, for example, offer utilities and ecosystem partners the ability to transform IoT sensor data to actionable information and perform control functions within the distributed network infrastructure.

Examples of deployed Fog applications include site asset management, energy monitoring, and protocol translation and street lighting.

Commitment to interoperability and open standards

Cisco has long been committed to network vendor interoperability. This means that with us, utilities are never locked into closed, proprietary technologies or protocols that support only a single service.

For more information Cisco's comprehensive security and utilities capabilities contact us at:

http://www.cisco.com/go/utilities

http://www.cisco.co.uk/security

Contact Power Networks Demonstration Centre:

62 Napier Road
Wardpark,
Cumbernauld,
Glasgow
G68 0EF

https://www.pndc.co.uk