Impregnable network defense for critical infrastructures

Protection with a defense-in-depth approach

Strategic White Paper

Securing critical infrastructures and their associated mission-critical communications is of utmost importance because they are the underpinnings of our modern society. From energy to transportation to public safety to mining, the advanced communications networks used by critical infrastructure operators carry data generated by electric grid IEDs, sensors, meters, surveillance cameras, LMR and 4G/LTE systems installed across the networks. These applications support unprecedented levels of

real-time monitoring and situational awareness, leading to improved operations efficiency, reliability, resiliency and safety. At the same time, cyber attacks increasingly threaten to disrupt critical infrastructure operations, making adoption of a defense-in-depth approach vital. This paper examines how critical infrastructure operators can identify, address and mitigate these threats with best practices and methodologies centered on the ITU-T X.805 security architecture using Nokia security capabilities – specifically an in-depth network security solution to address evolving security requirements.

NOKIA

Contents

Introduction: Securing critical infrastructures

Advanced communications networks are the keystones of critical infrastructures. Whether for energy, transportation, public safety or mining, operators rely on these networks to securely and reliably transport data generated by a multitude of applications to protect, control, monitor and operate the infrastructures all the time. Any communications disruption can incur immense economic loss and even jeopardize human lives. Hence, communications networks for critical infrastructures have become high-profile targets for individuals or groups seeking to disrupt or disable.

The prevalent use of information and communications technology (ICT) – particularly the shift toward a converged communications network infrastructure to support both mission-critical and non-mission-critical applications – improves operational efficiency substantially. However, it also introduces new vulnerabilities and increases the attack surface area.

Today, a wide range of security features in the defense tool box prevent and stop attacks. Operators can invest resources endlessly and in the end have a completely airtight, secure network but at an exorbitant cost to deploy and maintain. Therefore it is necessary for operators to understand the scope of protection rendered by the security features and ascertain the nature of the risks in their operating environment to attain the right balance.

A solution path: The ITU-T X.805 security architecture

A methodology-based approach to protecting critical infrastructure and networks provides a systematic means of assessing vulnerabilities and evaluating the level of

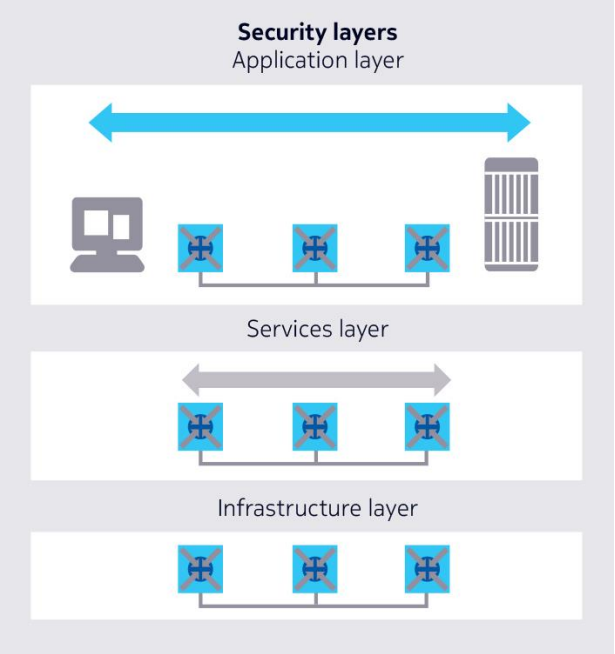
protection required. A framework must first be established to understand and evaluate risks and exposure. The ITU-T X.805 security architecture[1] presents a streamlined, simplified high-level threat model, enabling operators to assess network security and eliminate potential threats in complex environments, and it can be applied across network operations as well as in network management.

Nokia has contributed heavily to this architecture, which defines a hierarchy of network equipment and facility groupings into three layers (Figure 1):

- The **infrastructure layer**, which comprises basic communications network building blocks such as routers, switches, transport equipment and medium
- The **services layer**, which comprises network services or circuits that deliver data generated by applications, such as supervisory control and data acquisition (SCADA), land mobile radio (LMR) or closed circuit television (CCTV), end to end across the communications network
- The **application layer**, which comprises the devices, or simply known as endpoints, over which applications such as SCADA, video surveillance and IP telephony run. The endpoints could be a SCADA RTU, CCTV camera, SCADA server and video management system (VMS). An endpoint includes all associated hardware, software and firmware.

Figure 1. The three security layers in ITU-T X.805

[1] ITU-T X.805



Application layer security is also known as endpoint security, while infrastructure and services layer security are commonly called network security, which is the focus of this paper.

Major network security mechanisms

Table 1 maps major network security mechanisms to the X.805 layers that operate to protect the three data security properties:

- Confidentiality: prevention of unauthorized access to data
- Integrity: prevention of unauthorized modification or theft of data
- Availability: prevention of denial of authorized access to data

It is important to note that multiple mechanisms can be deployed jointly at different layers to form a defense-in-depth data protection. The rest of the paper will provide a highlight of the mechanisms.

Table 1. Network security mechanisms mapped to X.805 security layers

X.805 layer	Major defense mechanism	Defense purpose		
		Confidentiality	Integrity	Availability
Services layer	Multi-layer encryption	✓	✓	
	QoS-enabled service-aware firewall		✓	✓
	User security	✓	✓	✓
Infrastructure layer	Resilient IP/MPLS			✓
	Secure node	✓	✓	✓
	Intrusion detection	✓	✓	✓

Services security defense

Multi-layer encryption

An IP/MPLS network is already inherently secure due to its tunnel-based transport and VPN-based segregation. The optical and microwave transport have also been known to be a safe transmission medium. However, as the stakes are becoming higher than ever, the sophistication and frequency of attacks are rapidly rising. Hence it becomes crucial to encrypt the data. With encryption, even when the perpetrators tap into the communication channels, confidentiality and integrity are still protected.

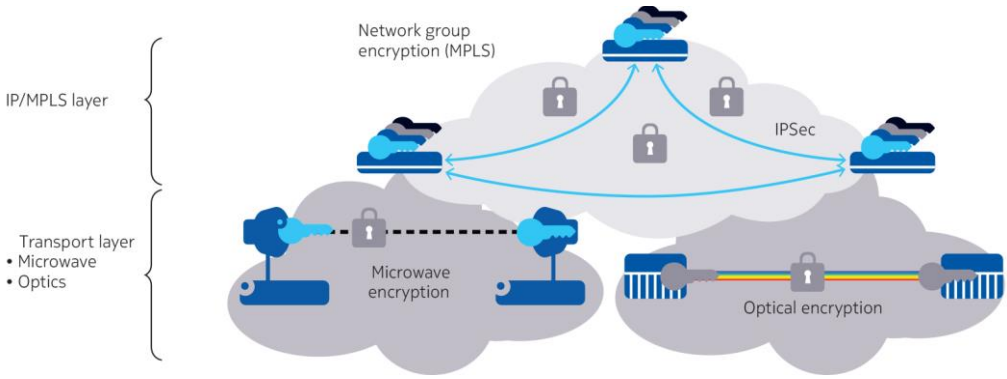
As the network is deployed with different architecture and transport technology, a multi-layer encryption capability (Figure 2) to not only encrypt at the IP layer as a typical IPSec gateway, but also at the MPLS[2] and transport layers[3], is important. This

[2] To read more about MPLS encryption (also known as network group encryption), please read Network group encryption: Seamless encryption for mission-critical networks

[3] For read more about transport encryption (also known as layer 1 encryption), please read Secure optical transport with the 1830 PSS Photonic Service Switch

flexibility allows operators to choose the most suitable encryption scheme based on a best-fit approach to attain complete end-to-end protection.

Figure 2. Multi-layer encryption



When compared with using traditional IPSec in an IP network for business communications, the use of encryption in a mission-critical network needs to support four unique attributes:

- **Multiprotocol encryption support**: Older applications such as SCADA and teleprotection remain crucial to critical infrastructure applications. Newer electric grid applications such as GOOSE/SV and AMI are Ethernet-based and IP-based respectively. Therefore it is necessary to be able to apply a commonly accepted encryption method such as AES-256 natively on multiple types of data to attain higher provisioning and operational efficiency, as well as ensure no quality of service (QoS) degradation (such as delay).
- **Optimal support for meshed tunnel**: With the emerging adoption of the Internet of Things (IoT), more devices and control points are deployed in the field. Therefore a multitude of secure meshed tunnels in the network is required to enable local communications, in addition to the secure tunnels to backhaul data to the network operating center (NOC) or command center (CC).
- **Centralized key management**: A centralized, redundant key management approach significantly reduces the complexity and effort in configuring and managing keys for the meshed tunnels, when compared with the traditional IPSec approach. A

centralized key management approach scales with greater ease and offers a single point of trust — one source for key generation, rotation and destruction.

- **Persistent secure tunnel connectivity**: As network connectivity is foundational to critical infrastructure operations, it is necessary for the secure tunnel to be up and running all the time, even in the unlikely disastrous event of redundant key server pair destruction. Seamless encryption at the MPLS layer also ensures tunnel connectivity in case of single or multi-fault failures.

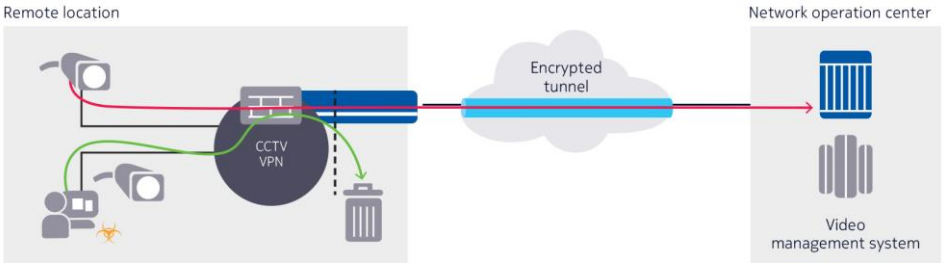
QoS-enabled service-aware firewall[4]

All devices in the remote sites and central NOC or CC need to be shielded from illicit access attempts to safeguard their integrity and availability, as well as protect them from being exploited as an attack launching pad. Consequently, a firewall is essential to inspect all incoming and outgoing traffic to permit only authorized flows. The firewall can also limit the number and volume of communications sessions to stop attackers from hijacking legitimate sessions. As critical communications are typically conducted in segregated and encrypted VPN services, the firewall needs to be service-aware and operate seamlessly with the encrypted label switched path (LSP) tunnel (Figure 3).

Since the firewall operates in a session-aware, stateful manner, there are also concerns about its impact on QoS for real-time applications. With the latest hardware acceleration, an IP/MPLS router-based firewall can efficiently operate in conjunction with data forwarding and encryption operation with no network performance degradation.

[4] To read more on firewalls for mission-critical networks, please read Nokia 7705 Service Aggregation Router: Security overview for mission-critical networks

Figure 3. Service-aware firewall deployment

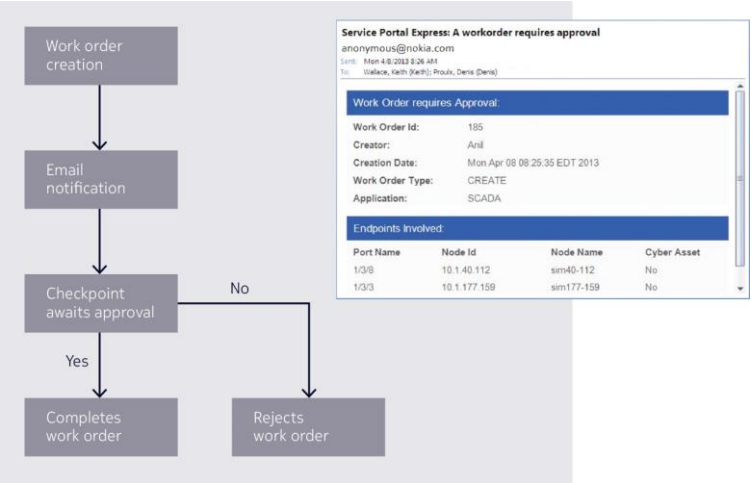


User security

Being human is both the strength and weakness in cyber defense. On one hand, a discerning mind can supplement security technology to spot a network anomaly and stop an attack. On the other hand, a significant percentage of security breaches can be traced back to human errors — from lack of compliance to unintentional configuration error to identify theft. When such a security breach occurs, overall application security is violated.

A role-based user profile can be tailored to render the appropriate span of control of the network and scope of command of network capability. As an example, an application user is given only privileges to administer network services, but not network infrastructure configuration, while a network engineer, the reverse. This is an effective way to mitigate the possible damage that can be inflicted by a user, advertently or inadvertently. Furthermore, operators can impose checkpoints when network services are created, modified or deleted. A checkpoint is a work order is checked by an authorized person (Figure 4). Even in the case of user identity theft, an unauthorized work order would be caught and stopped. Furthermore, all user actions are logged for security audit and investigation purposes.

Figure 4. Work flow checkpoint



Infrastructure security defense

Resilient network infrastructure

A resilient network infrastructure is pivotal to attain uninterrupted service availability. Therefore a network must withstand equipment, connectivity or other failures, intentional or accidental. With well-planned and adequate physical connectivity, an IP/MPLS network can withstand even multi-fault events to ensure data flow is not stopped. Its comprehensive recovery mechanism, including fast re-route and standby LSP (Figure 5) as well as pseudowire redundancy (Figure 6), ensures that traffic can be restored even when the network, the NOC or CC, suffers from disruptions. Similarly, the underlying physical network should be built to withstand equipment failures or physical disruption. Design practices that utilize redundant hardware, automatic protection switching and diverse transmission paths have long been common in communications networks. Optical transmission systems utilize a number of protection schemes to protect the physical link, including 1:1, 1+1, 1:N, ring or mesh configurations. Working and protection paths are commonly placed along different physical paths to avoid single points of failure. Power sources usually include integral

back-up mechanisms. These practices ensure service resiliency regardless of whether the root cause is equipment failure, natural disaster or intentional attack.

Figure 5. MPLS resiliency protects against multipoint network disruption

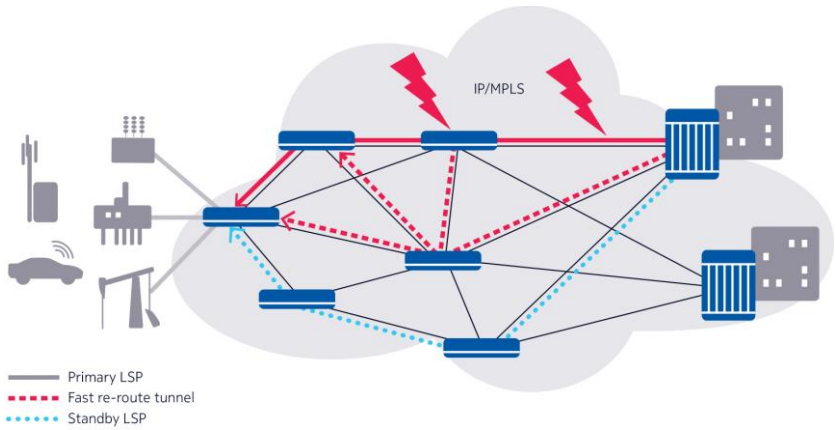
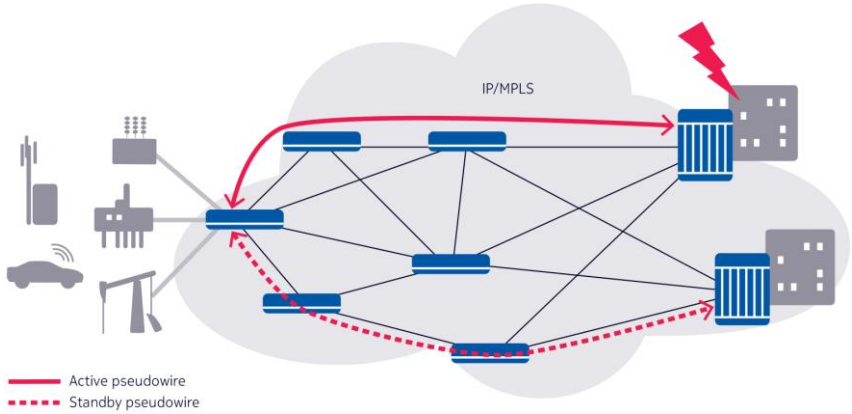


Figure 6. Pseudowire redundancy provides geo-protection for NOC/CC



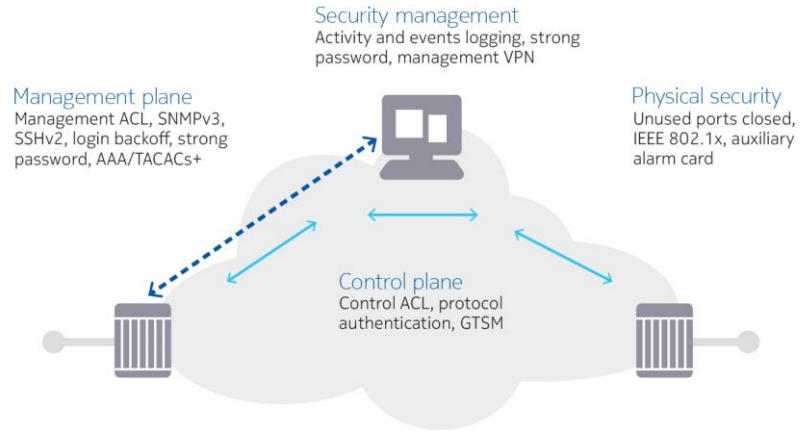
Secure node

A secure node is fundamental to provide a network with safe and reliable connectivity to critical applications and to ensure network topology confidentiality as well as data integrity and availability. Therefore it is crucial to prevent attackers from snooping at or altering nodal configurations or exploiting them as a launching pad to compromise endpoints and bring down applications. Consequently, the node's control plane, management plane and physical ports need to be fortified to keep attackers at bay.

A well-proven strategy is to minimize the node's attack surface is by closing all communications ports (physical or TCP/UDP) in a tightly secure mode. This mode leaves open only essential logical and physical ports needed by the control and management planes and the services layer.

Moreover, in order to monitor and spot suspicious activity, all management activity and security events should be logged and monitored. Figure 7 provides an overview of these various security dimensions.

Figure 7. Fortifying a network node



Intrusion detection

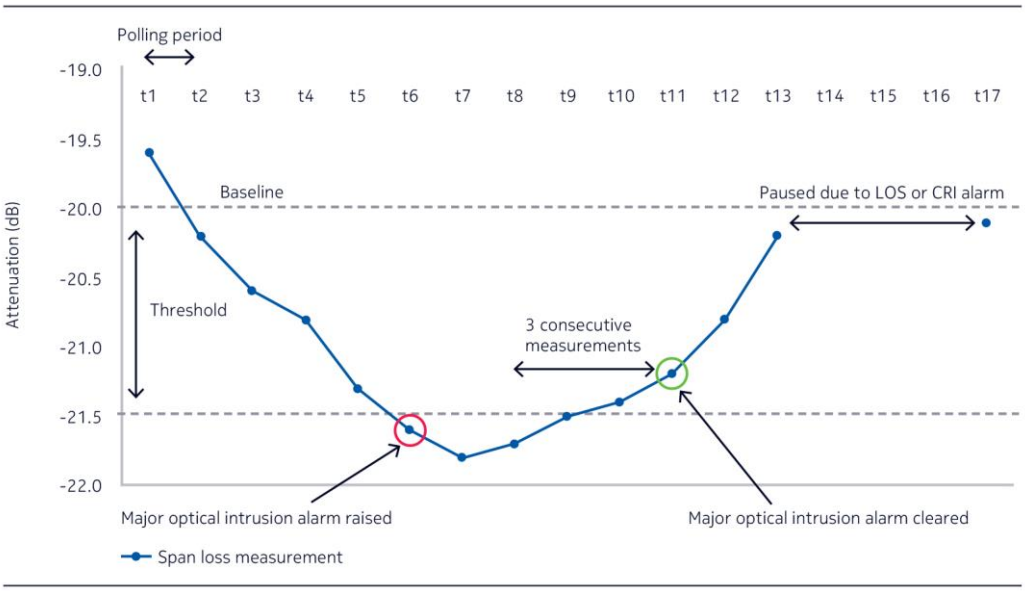
In addition to detecting intrusion at the packet or session layer by router, firewall and other security appliance, physical intrusion detection at the transport physical layer is equally crucial to protect overall data security. In the past, fiber optics transmission was deemed to be secure. However, with the right tools, fiber tapping is now surprisingly easy to perform.[5] While techniques such as optical encryption can

5 "Guide to Fiber Optics and Premises Cabling," The Fiber Optic Association, Inc.

safeguard data confidentiality and integrity, the perpetrators can still lurk in the network without being detected.

By detecting optical signal loss and identifying its location through techniques such as OTDR, the network can effectively scout out the presence of intrusion and even its location. That this capability used to be available only in specialized test equipment limits its applicability to regular fiber maintenance and troubleshooting. However, as new-generation optical platforms start to integrate such capability natively, operators can now monitor the whole network continuously for intrusion (Figure 8).

Figure 8. Network-wide intrusion detection by network manager



Summary

The operational environment of critical infrastructure is evolving in terms of threats, technologies and compliance. Effective protection of critical assets requires a layered defense-in-depth apXproach, employing a range of security mechanisms jointly at different security layers based on the ITU-T X.805 security architecture. This structured approach enables operators to lay a robust foundation for their security guidelines and best practices.

Nokia has real-world expertise developing field-proven cybersecurity best practices with operators. Our industry-leading mission-critical networks solutions not only deliver the required network reliability, performance and scalability, they also serve as a bulwark defending against security threats and attacks. Nokia can contribute significantly to your efforts to protect critical infrastructure and address regulatory requirements.

Acronyms

AAA	Authentication, Authorization and Accounting
ACL	access control list
AES	Advanced Encryption Standard
AMI	Amazon Machine Image
CC	command center
CCTV	closed circuit television
GOOSE/SV	Generic Object Oriented Substation Event/Sampled Values
ICT	information and communications technology
IED	intelligent edge device
IPSec	Internet Protocol Security
LMR	Land Mobile Radio
LSP	label switched path
LTE	Long Term Evolution
MPLS	Multiprotocol Label Switching
NGE	Network Group Encryption
NOC	network operating center
QoS	quality of service
OTDR	optical time-domain reflection

RTU	remote terminal unit
SCADA	supervisory control and data acquisition
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TACACS+	Terminal Access Controller Access-Control System Plus
VPN	virtual private network

Nokia Oyj
Karaportti 3
FI-02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Product code: PR1603018805EN