Secured Edge Node Technical Compliance Register: critical infrastructure protection cyber secure routers

SECURED EDGE NODE TECHNICAL COMPLIANCE REGISTER: CRITICAL INFRASTRUCTURE PROTECTION CYBER SECURE ROUTERS

EXECUTIVE SUMMARY

This document serves as the official Technical Compliance Register for the Sentinel-ISR (Intelligent Security Router) series, a family of critical infrastructure protection (CIP) cyber secure routers engineered for the most demanding operational technology (OT) and information technology (IT) convergence environments. The Sentinel-ISR platform is architected to meet and exceed the stringent requirements of NERC CIP, IEC 62443, and NIST SP 800-82 frameworks, providing a ruggedized, high-performance routing solution that ensures the confidentiality, integrity, and availability of essential network services.

The Sentinel-ISR is not merely a router; it is a comprehensive security enforcement point. It integrates line-rate, hardware-accelerated encryption, advanced access control lists (ACLs), and deep packet inspection (DPI) capabilities directly into its forwarding pipeline. This design eliminates performance bottlenecks commonly associated with software-based security appliances, guaranteeing wire-speed throughput for both clear-text and

encrypted traffic. The platform is ideal for use cases including substation automation, smart grid communications, pipeline monitoring, railway signaling, and other mission-critical industrial and governmental networks.

SYSTEM HARDWARE TOPOLOGY & CHASSIS DESIGN

The Sentinel-ISR architecture is built upon a dual-plane, non-blocking switching fabric that separates the control and data planes at the hardware level. The system is available in two primary chassis configurations: the compact Sentinel-ISR 100 (1RU) for edge and access deployments, and the high-capacity Sentinel-ISR 3000 (3RU) for aggregation and core edge roles. Both chassis share a common modular design philosophy, emphasizing field-replaceable components and forward compatibility.

At the heart of the system is the central backplane, which provides a dedicated 800 Gbps (ISR 100) / 3.2 Tbps (ISR 3000) of non-blocking switching capacity. This backplane utilizes a high-speed serial interconnect (HSSI) that minimizes latency and jitter, critical for real-time control applications. The physical design incorporates advanced thermal management with front-to-back airflow, multiple high-efficiency fan trays, and an electromagnetic interference (EMI) shielding that exceeds FCC Class A and CISPR 32 standards.

DATA & CONTROL PLANE CAPABILITIES

The Sentinel-ISR implements a strict architectural separation between the data forwarding plane and the system control plane. The data plane is powered by a custom-designed, fifth-generation network processor (NPU) that integrates a dedicated security co-processor. This NPU is responsible for all packet forwarding, QoS queuing, and security operations (IPsec, MACsec, ACL filtering) at line rates up to 100 Gbps per port. The security co-processor includes hardware-based random number generation (HRNG) and secure key storage, meeting FIPS 140-3 Level 3 physical security requirements for cryptographic modules.

The control plane is managed by a high-availability dual-core x86 processor complex running a hardened, real-time Linux operating system. This CPU

complex handles all routing protocol processing (OSPF, BGP, IS-IS), network management functions (SNMP, NETCONF, RESTCONF), and orchestration tasks. To ensure system integrity, the control plane is isolated from the data plane via a secure inter-process communication (IPC) channel, preventing a compromised control plane from affecting forwarding operations. All software images are cryptographically signed, and the system supports secure boot (UEFI Secure Boot) to establish a root of trust from power-on.

SECURITY POSITIONING & LINE-RATE ENCRYPTION

Network security is the foundational pillar of the Sentinel-ISR. The platform is designed to protect critical infrastructure against both external cyber threats and internal malicious actors. Key security features include:

Hardware-Accelerated Encryption: The integrated security co-processor supports IPsec (ESP/AH) with cipher suites including AES-GCM-128/256, AES-CBC-128/256, and ChaCha20-Poly1305. MACsec (IEEE 802.1AE) is supported on all Ethernet ports, providing link-layer encryption and integrity. The co-processor can sustain line-rate encryption for all packet sizes, ensuring that security does not come at the cost of performance.

Role-Based Access Control (RBAC): Administration is governed by TACACS+

and RADIUS, with granular privilege levels. The platform supports multi-factor authentication (MFA) for local and remote management access, and all administrative sessions are encrypted via SSHv2 or TLS 1.3.

Anomaly Detection & DPI: The data plane includes a deep packet inspection engine capable of analyzing traffic patterns for known attack signatures and protocol anomalies. This engine can be dynamically updated with new threat intelligence feeds, enabling proactive threat mitigation.

PHYSICAL TAMPER-RESISTANCE & RESILIENCY

The Sentinel-ISR is engineered for physical security and operational resilience. The chassis features tamper-evident seals and a physical lockable bezel to prevent unauthorized access to internal components. The system incorporates a Trusted Platform Module (TPM) 2.0 for secure storage of cryptographic keys and platform measurements. In the event of a physical breach, the system can be configured to zeroize all stored keys and sensitive data automatically.

For high-availability environments, the platform supports 1+1 redundant power supplies (AC or DC), N+1 fan redundancy, and a hot-swappable dual-route processor (RP) configuration. The modular route processors enable in-service software upgrades (ISSU) and provide stateful switchover (SSO) and

non-stop routing (NSR), ensuring sub-second failover and zero packet loss during maintenance events.

DETAILED PARAMETERS & PERFORMANCE SPECIFICATIONS

The following table provides the comprehensive technical specifications for the Sentinel-ISR 100 and Sentinel-ISR 3000 platforms. All performance metrics are measured under typical operational conditions with a 50/50 mix of UDP and TCP traffic using 64-byte and 1518-byte frame sizes.

Parameter	**Specification**
Form Factor	Sentinel-ISR 100: 1RU (19-inch) / Sentinel-ISR 3000: 3RU (19-inch)
Switching Capacity (Non-Blocking)	ISR 100: 800 Gbps / ISR 3000: 3.2 Tbps
Forwarding Rate (64-byte packets)	ISR 100: 600 Mpps / ISR 3000: 2.4 Bpps
IPsec Throughput (AES-GCM-256)	ISR 100: 75 Gbps / ISR 3000: 300 Gbps
MACsec Throughput	ISR 100: 100 Gbps / ISR 3000: 400 Gbps
Interface Types (Pluggable)	SFP, SFP+, SFP28, QSFP28 (copper and fiber options up to 400G)
Power Supply	Dual, 1+1 Redundant Hot-Swappable: 100-240V AC (50/60Hz) or -48V DC

Typical Power Consumption	ISR 100: 275W / ISR 3000: 850W
Operating Temperature Range	-40°C to +70°C (Industrial Grade)
Storage Temperature Range	-40°C to +85°C
Relative Humidity (Non-condensing)	5% to 95%
Packet Buffer Memory	ISR 100: 32 GB / ISR 3000: 128 GB
Control Plane CPU	Dual-core Intel Xeon D-2100 series (ISR 100) / Octal-core Intel Xeon Silver (ISR 3000)
System Memory (Control Plane)	ISR 100: 16 GB DDR4 ECC / ISR 3000: 64 GB DDR4 ECC
Flash Storage (Internal)	ISR 100: 2x 240 GB M.2 SSD (RAID 1) / ISR 3000: 2x 480 GB M.2 SSD (RAID 1)
Management Ports	1x 10/100/1000Base-T Dedicated, 1x RJ45 Console, 1x USB-C
Routing Protocols	OSPFv2/v3, BGP-4, IS-IS, RIPv2, PIM-SM, MPLS, LDP
Security Protocols	IPsec (IKEv1/v2), MACsec, SSL/TLS, SSHv2, SNMPv3
High Availability	SSO, NSR, ISSU, BFD (Bidirectional Forwarding Detection)
Clock Synchronization	IEEE 1588-2008 (PTPv2), NTPv4
Weight (Fully Loaded)	ISR 100: 12 kg / ISR 3000: 34 kg

MTBF (at 40°C)	ISR 100: >280,000 hours / ISR 3000: >220,000 hours (Telcordia SR-332)

COMPLIANCE & STANDARDS CERTIFICATIONS MATRIX

The Sentinel-ISR series has undergone rigorous third-party validation and testing to ensure compliance with global regulatory and industry-specific standards. The complete list of certifications is detailed below:

Security & Information Assurance:

- NERC CIP-002 through CIP-011 (Critical Infrastructure Protection standards for the bulk electric system)
- IEC 62443-4-2 (Security for Industrial Automation and Control Systems - Part 4-2: Technical security requirements for IACS components)
- NIST SP 800-82 (Guide to Industrial Control Systems Security)
- FIPS 140-3 (Cryptographic Module Validation Program, overall Level 2, physical security Level 3)
- DoDIN APL (Department of Defense Information Network Approved Products List - pending)

Environmental & Physical:

- ETSI EN 300 019 (Class 3.4 for extended environmental conditions)

- MIL-STD-810H (Method 501.7 High Temperature, Method 502.7 Low Temperature, Method 507.6 Humidity, Method 514.8 Vibration, Method 516.8 Shock)

- IEEE 1613 (Environmental and Testing Requirements for Communications Networking Devices in Electric Power Substations)

- IEC 61850-3 (Communications networks and systems for power utility automation - General requirements)

Electromagnetic Compatibility (EMC) & Safety:

- FCC Part 15 (Class A)

- ICES-003 (Industry Canada)

- EN 55032 / CISPR 32 (EMI)

- EN 55035 / CISPR 35 (Immunity)

- UL 60950-1 / IEC 62368-1 (Safety)

- CE Marking (EU Directives)

LIFECYCLE ASSURANCE (MTBF & SUPPORT)

The Sentinel-ISR platform is backed by a comprehensive lifecycle assurance program. The calculated Mean Time Between Failures (MTBF) for the

Sentinel-ISR 100 is > 280,000 hours at 40 °C ambient temperature, and > 220,000 hours for the Sentinel-ISR 3000, according to Telcordia SR-332, Issue 4. The system is designed for a 10-year service life, with a minimum 7-year end-of-sale (EOS) commitment and a 10-year end-of-life (EOL) support period from the date of product introduction. This long-term support ensures network stability and protects capital investments.

Our global support infrastructure provides 24/7/365 technical assistance, with advanced replacement service (4-hour response) and on-site field engineering available for critical accounts. All support services are delivered by engineers certified in both networking and industrial control system security.

TARGET NETWORK TOPOLOGIES & DEPLOYMENT ARCHITECTURE

The Sentinel-ISR is designed to serve as a secure aggregation and routing node at the edge of critical infrastructure networks. Common deployment architectures include:

Perimeter Defense for Industrial Control Systems: Deployed as a secure gateway between the enterprise IT network and the industrial OT network, enforcing strict zone-based firewalling and deep inspection of protocols such as Modbus/TCP, DNP3, IEC 61850 (GOOSE, SV), and OPC UA.

Substation Automation & Smart Grid Backhaul: The router interfaces with intelligent electronic devices (IEDs), remote terminal units (RTUs), and phasor measurement units (PMUs), providing deterministic latency for mission-critical trip and protection signals. Its support for Precision Time Protocol (PTP) IEEE 1588-2008 enables sub-microsecond time synchronization across the distribution network.

Remote Site Connectivity for Oil & Gas: The ruggedized design and support for serial interfaces (RS-232/422/485) via field-replaceable pluggable modules make it ideal for remote pipeline and wellhead monitoring. The built-in hardware encryption ensures secure backhaul over satellite or 4G/5G LTE cellular links.

Government & Defense Networks: The platform meets stringent security and anti-tamper requirements, making it suitable for tactical edge deployments and sensitive but unclassified (SBU) networks requiring high-assurance IPsec and MACsec.


SENTINEL-ISR