

Solution Brief

SecFlow with SD-IoT Technology

Mission-critical communications challenges

Critical Infrastructure (CI) companies, such as power utilities, oil and gas companies, transportation, water utilities and public safety agencies are facing numerous telecommunications or connectivity challenges:

- **Resiliency and Redundancy:** mission-critical systems need to be resilient to withstand natural disasters, physical attacks or vandalism, and other disruptions. Redundancy, both in terms of communication channels and data centers is crucial to maintain continuous services and uninterrupted operations.
- **Modernization:** Rapid advancements in technology present new, smaller and cost-effective solutions that have been replacing legacy Supervisory Control And Data Acquisition (SCADA) systems widely deployed in CI operational technology (OT) networks. Modern IoT and Industrial IoT (IIoT) devices are now available for modernizing infrastructure and extending monitoring and supervision to unmanaged parts of CI equipment. These devices need to be aggregated and connected, with special attention to systems in which legacy sensors and controllers coexist with new ones.
- **Cybersecurity Threats:** As CI infrastructure becomes increasingly interconnected, it is also more vulnerable to cyberattacks, as the attack surface grows exponentially. Ensuring secure communications and connectivity is paramount, as a breach can have severe and even life-threatening consequences.
- **Regulatory Compliance:** Because of the above challenges, CI companies are also subject to increased regulation that dictates how data should be handled.

To address these challenges, CI companies are using secure and reliable fiber networks as their main OT network communication media. Where fiber is not available or too costly to deploy, they are looking into 4G/LTE/5G technologies to connect their assets. They are also looking for new communications gateways that employ encryption technologies, firewalls, and other functionalities to secure operational data. Such gateways should also provide connectivity from remote sites towards the central command and control servers, both for existing SCADA systems and for next-gen devices using new protocols such as IEC 61850 GOOSE, MMS and SV protocols.

Meeting ALL these requirements with the SAME gateway, however, poses the biggest challenge for CI organizations.

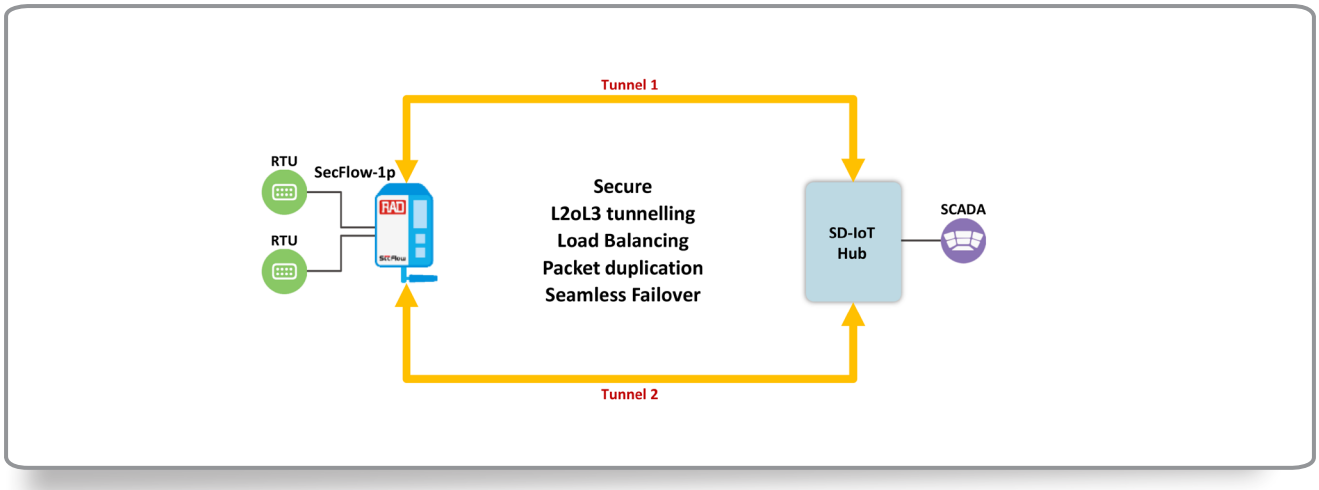
RAD's SecFlow IoT Gateway with SD-IoT

RAD's SecFlow IoT Gateway supports SD-IoT technology to address CI challenges and ensure resilient, secure, and reliable connectivity. It enables existing mission-critical applications, as well as offering the flexibility to support future CI requirements.

PulseSupply
pulsesupply.com

RAD
Your Network's Edge®

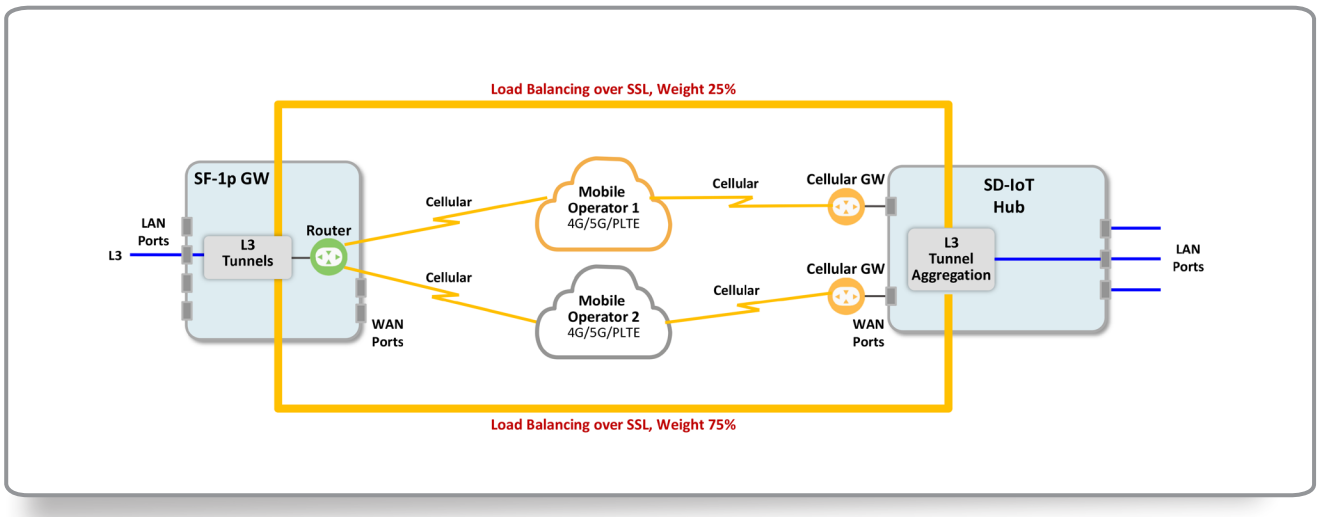
Solution Brief
SecFlow with SD-IoT Technology



Let's look at the different capabilities offered by RAD's SecFlow-1p:

Layer 3 Load Balancing

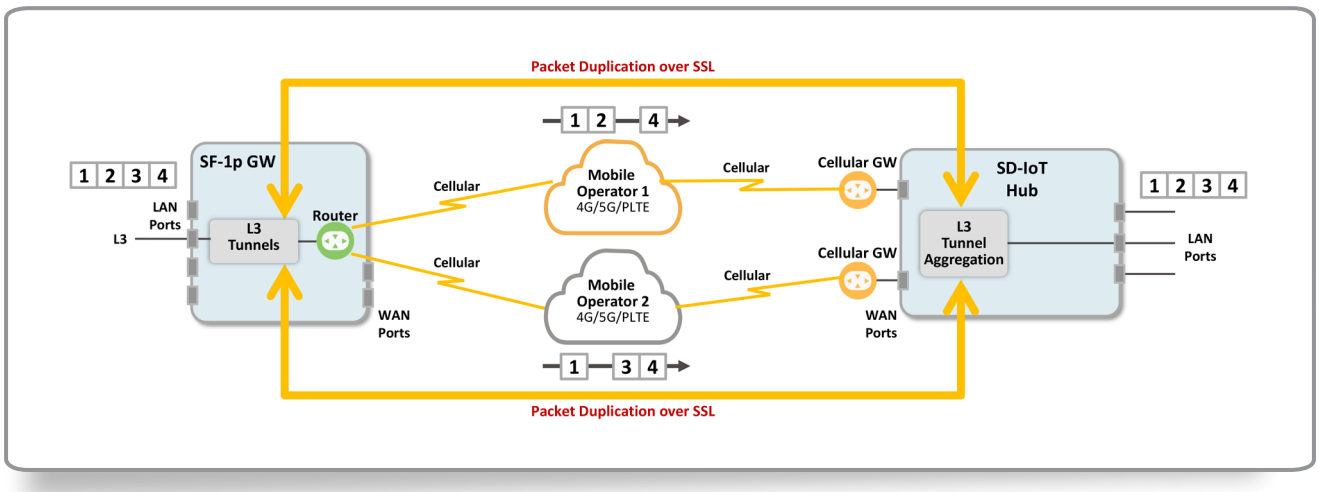
The SecFlow-1p with SD-IoT technology distributes L3 traffic packet-by-packet over several links. The weight of each link can be configured, in case one of the networks provides lower bandwidth than the other. Packet sequencing eliminates out-of-order packets on the receiver end.



Benefits:

- **Increased bandwidth availability** by distributing traffic over two separated networks.
- **Fast resiliency** compared to standard routing protocols, as traffic is seamlessly moved to another active network.
- **Secure transport** as ALL packets are encrypted using TLS

This operational mode duplicates L3 packets and transmits them over multiple networks. In case one network loses a packet, the packet will arrive at the SD-IoT Hub via another link, thereby reducing packet loss to ZERO. Again, packet sequencing eliminates out-of-order packets on the receiver end.



Benefits:

- **Uninterrupted operations** with ZERO packet loss: Packets are duplicated over two links and even if packets are lost in one link, they are re-inserted into the packet flow
- **Secure transport** as ALL packets are encrypted using TLS

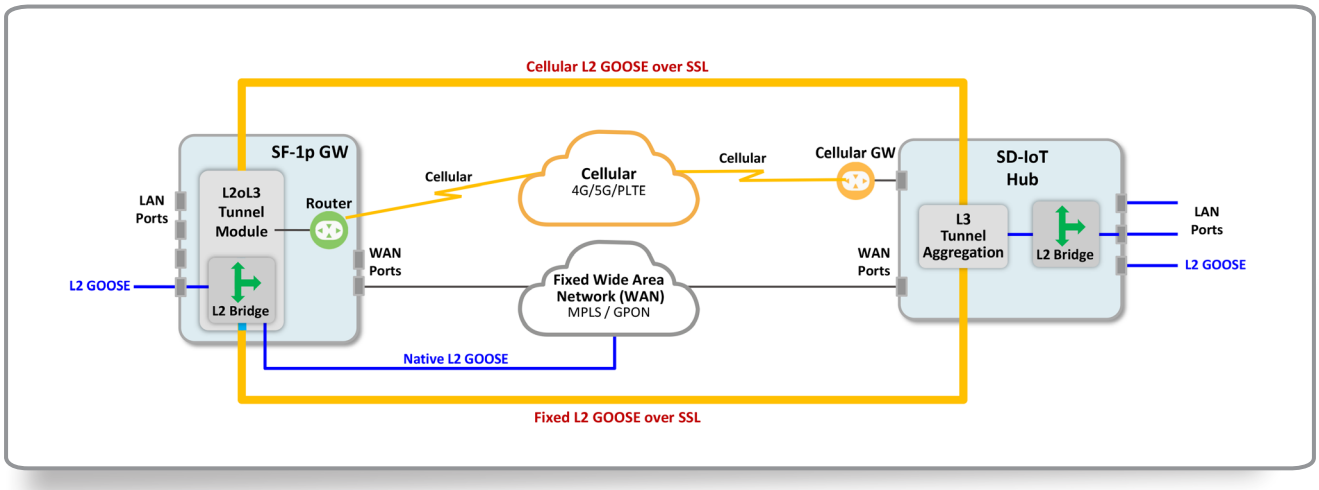
Layer 2 over Layer 3 Tunneling

Another common challenge for many CI operators is the need to transport L2 traffic over mobile networks, such as 4G/LTE or 5G, which support only L3 traffic. RAD's SecFlow-1p encapsulates L2 traffic over L3, then encrypts the packets before transmitting them over the cellular networks.

A typical use case for this would be a power utility transitioning to IEC 61850-based systems.

IEC 61850 is being increasingly adopted by power utilities, requiring them to transport IEC 61850 GOOSE traffic from one electrical substation to several others, and to connect new Distributed Energy Resources (DERs) to the electrical grid. IEC 61850 GOOSE devices transmit L2 multicast packets between Remote Termination Units (RTUs) and Intelligent Electronic Devices (IEDs).

Solution Brief
SecFlow with SD-IoT Technology



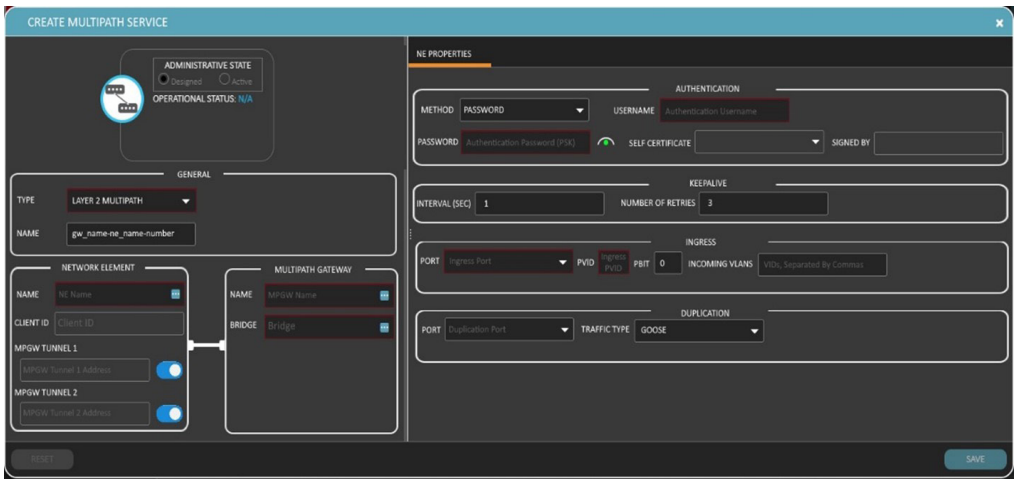
A virtual bridge in RAD's SecFlow-1p IoT gateway receives these packets and forwards them to the SD-IoT client, which encapsulates the L2 packets over L3, encrypts them using TLS and transmits them over the cellular link (or any other WAN link available). If the SecFlow-1p is also connected to an existing fiber network (G-PON, SDH, SONET, MPLS), the packets are also forwarded to this native interface, without a L3 encapsulation for fast transmission to neighboring substations.

Benefits:

- **Fast path** of native GOOSE transmission over fiber network when available.
- **Secure GOOSE** transmission over 4G/LTE/5G cellular networks, either as a primary link or as a backup connection if the fiber network is out of service.
- **VLAN awareness** of GOOSE frames ensuring connectivity to neighboring substations based on VLAN IDs.

Managing the SecFlow-1p IoT Gateway

The SD-IoT client on the SecFlow-1p, as well as the SD-IoT Hub located in central control are managed by CLI, REST or RAD's RADview network management platform. RADview presents a full and friendly GUI to configure end-to-end services and monitor all services and circuits.





Solution Brief
SecFlow with SD-IoT Technology

Additional technical data:

SecFlow-1p with SD-IoT Client	
SD-IoT client is embedded in the SecFlow-1p and can be activated on demand. This feature requires a Multipath Hub in the hub site. See SecFlow-1p **Data Sheet** for additional information.	
SD-IoT Hub	
• SD-IoT Hub aggregates tunnels from the SecFlow-1p SD-IoT client. It runs on Intel servers as bare metal or on virtual machines. Services can be configured via CLI or via REST APIs. It is supported by RADview, which can configure end-to-end services from multiple SecFlow-1p IoT Gateways towards the SD-IoT Hub. • SD-IoT Hub system requirements: - Single or multi-sockets Intel® Xeon® and Atom® processor - Cores: 28 minimum - RAM: 64G minimum - Storage: 128G minimum *CPU type, number of cores are dependent on number of tunnels required.* SD-IoT Hub system deployment: - Linux Ubuntu - Installed on bare metal or VMs - Update/rollback support - Support of resilient SD-IoT Hubs for high availability - Scalability: Up to 10,000 tunnels / 5000 clients *(see HW recommendation as per number of tunnels)*	
Tunneling Modes	
- L3 load sharing (with weight per link) - L3 packet duplication - L2oL3 tunnels	
Layer 2	
- VLAN aware Ethernet bridge - VLAN (802.1Q)	
Encryption schemes	
- TLS - IKE v1/v2 pre-shared keys or X509 certificates - Encryption: – 3DES, AES-CBC/GCM (128, 192, 256) - Hash: – MD-5, SHA-1, SHA-2 (256, 384, 512) AES-XCBC (128) - Key management: – RSA, DH MODP groups 1 (768 bits), 2 (1024 bits), 5 (1536 bits) and 14 (2048 bits), DH PF	
Quality of Service	
- Class-based QoS	
Key RADview features	
- End-to-End VPN configuration - SecFlow-1p tunnel configuration - SD-IoT Hub tunnel configuration - L2 bridge and VLAN configuration - Tunnel status and statistics	



Solution Brief
SecFlow with SD-IoT Technology

SecFlow-1p with SD-IoT is ideal for power utility operators as well as communications service providers offering IoT services.

RAD's SecFlow-1p with SD-IoT Technology – Highlights:

- Software-defined capability, running on any hardware, highly flexible and easy to deploy.
- Secure backup and failover for main fiber/GPON connectivity – critical service availability assurance – over LTE/4G/5G mobile services.
- Optional second LTE/5G mobile service for secure mission-critical services.
- Load balancing and link duplication ensuring ZERO packet loss and continuous critical ser-vices availability.
- Uninterrupted, secured and protected operational services.
- Seamless failover capabilities for Layer2 SCADA, IEC 61850, IoT mission-critical services.

Learn more about RAD's SecFlow here»

Pulse Supply
909 Ridgebrook Road.,Sparks,Maryland
21152,USA TEL : +1-410-583-1701
FAX : +1-410-583-1704
E-mail: sales@pulsesupply.com
https://www.pulsesupply.com/rad

www.pulsesupply.com/rad

Your Network's Edge®

Specifications are subject to change without prior notification. The RAD name, logo and logotype, are registered trademarks of RAD Data Communications Ltd. RAD product names are trademarks of RAD Data Communications Ltd. ©2025 RAD Data Communications. All rights reserved. Version 05/25.