

DATASHEET

Connectivity Aggregation

Software that combines cellular, satellite, Wi-Fi, and other IP networks into one resilient link, so your machines keep working when individual connections degrade.

PRODUCT	PRODUCT TYPE	AVAILABILITY	DOCUMENT ID
Connectivity Aggregation	Software	Q4 2026	DS-CONNAGG

01 Overview

Connectivity Aggregation combines every network path a machine can reach into a single, resilient, encrypted link. It spreads traffic across all of the underlying networks at the same time, based on current network conditions and on the latency, reliability, and bandwidth each type of traffic needs. Individual connections can degrade. The aggregated link does not.

You run it on your own hardware, over the consumer networks and network hardware you already use. Each connection runs the software on both ends, usually on a mobile machine and at an operator station, or on two machines that communicate with each other.

The problem it solves

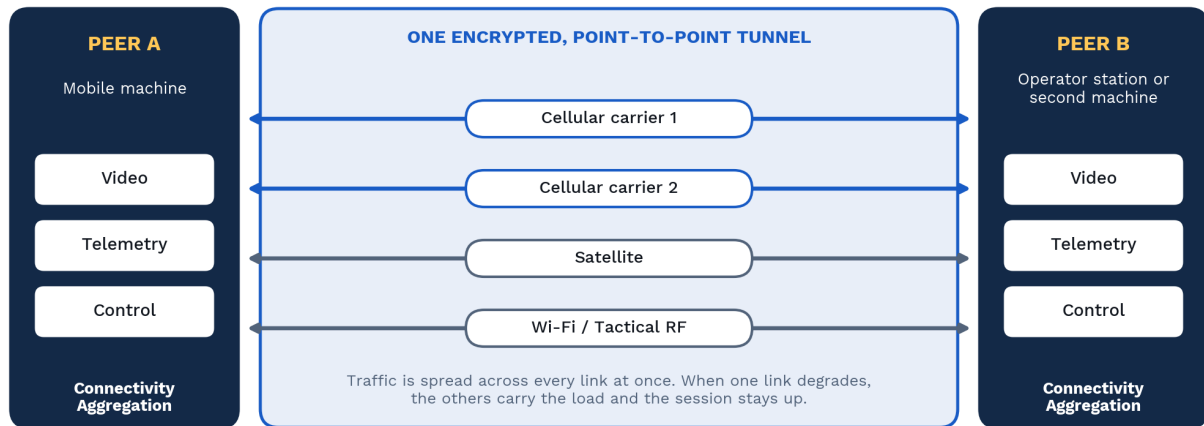
Network reliability varies, and no two providers have coverage gaps in the same places. Safety systems are built to fail safe, so a machine that relies on one network stops whenever that link times out. Adding more networks helps only if something manages them well.

- ◆ **Switching networks stops the work.** When you operate vehicles remotely over long distances, switching between communication channels by hand each time a link becomes unavailable or unreliable is slow and inconvenient, and the machine stops while it happens.
- ◆ **Bonding and prioritization are hard to manage together.** Your machines send several types of traffic, such as video, telemetry and control, over several network links. Managing link bonding and stream prioritization at the same time is difficult.
- ◆ **More networks shouldn't mean wasted bandwidth or weakest-link reliability.** You want to use every available network without spending bandwidth you don't need, and without being held to the reliability of the weakest link.
- ◆ **One network means more stops.** When your machines depend on a single network, every gap in its coverage or drop in quality can trigger a protective stop.

Typical applications

- Remote operation of vehicles and machines over long distances
- Defense and field robotics
- Autonomous vehicles and mobile robots that cross coverage gaps
- Sites where one provider's coverage does not match the work area
- Bandwidth-heavy video alongside latency-sensitive control and telemetry

How Connectivity Aggregation works: one tunnel across every available link



Your applications send data into a tunnel, and Connectivity Aggregation delivers it to the receiving application with the reliability and priority you configured, as if the two applications were connected directly. Link management, encryption, key management, and peer discovery are handled for you.

02

Key Features

Full active-active aggregation

Uses all available links at once, with no switchover time like active-standby failover systems, and opportunistically uses extra bandwidth as conditions permit.

Bond every path the machine can reach

Multiple cellular carriers, satellite, Wi-Fi, Ethernet, tactical RF, or any other IP network on hand. No proprietary hardware or custom cellular links required.

Link-state aware

Continuously evaluates each link's bandwidth, latency, and other metrics. When a path starts to degrade, it re-evaluates the transmission strategy and moves traffic before the operator notices.

Traffic classes that cooperate

Multiple tunnels schedule together instead of competing. Video can preempt telemetry, and control signals can carry more redundancy than operator audio.

Your tradeoff to make

Choose the point on the latency, reliability, and bandwidth curve for each class of traffic, rather than accepting one setting for everything.

Detailed link metrics

Metrics and logs for every tunnel, so you can validate behavior, investigate a bad shift, and tune for whatever objective your deployment cares about.

Secure by default

All traffic is encrypted end to end. Endpoints verify each other with asymmetric cryptography, so only the intended recipient can read the data.

Works through NAT and CGNAT

Connects hosts behind NAT or carrier-grade NAT, common on cellular and satellite networks, without router or firewall changes. Peers find each other automatically by public key.

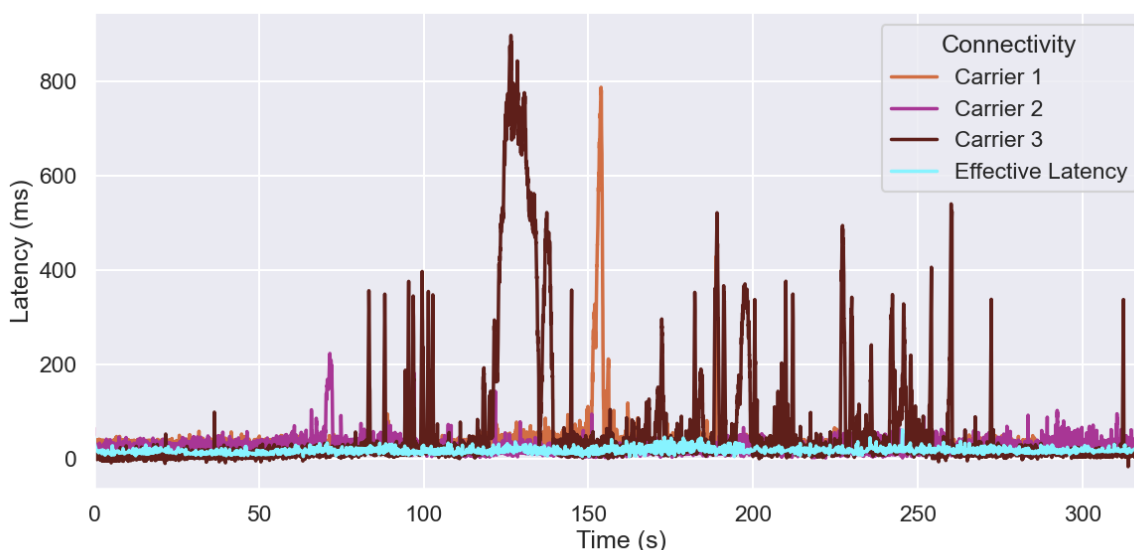
Choosing a tradeoff

Connectivity Aggregation splits data into shards and spreads them across the available links. The configuration you choose sets where each class of traffic sits between lowest latency and highest bandwidth.

GOAL	WHAT IT DOES	RESULT
Minimize latency	Sends shards so the 95th-percentile latency is as low as possible.	Lowest latency; lowest effective bandwidth.
Balanced	Trades some latency for additional bandwidth.	A middle point you tune to your needs.
Maximize bandwidth	Uses the combined capacity of all links.	Highest effective bandwidth; highest effective latency.

Reliability is tunable too. For example, you can send additional redundant shards for control traffic.

Latency of three individual carrier links compared with the effective latency of the aggregated link



OPERATIONAL BENEFITS

- ✓ Fewer nuisance safety stops and less unplanned downtime.
- ✓ Larger effective work area from the same site coverage.
- ✓ Fewer manual retrievals from dead zones.
- ✓ Lower control latency than VPN-based solutions.

DEPLOYMENT BENEFITS

- ◆ Operator trust that the machine will not drop mid-task.
- ◆ Deployments that travel to environments you do not control.
- ◆ One integration instead of a per-site network project.
- ◆ Bandwidth-hungry streams without starving latency-sensitive ones.

IMPORTANT

Connectivity Aggregation is a networking product, not a safety function. Video carried over Connectivity Aggregation is not safety-rated video.

03**Specifications****SUPPORTED NETWORKS**

Tested network types	Cellular (multiple carriers), satellite, Wi-Fi, Ethernet, tactical RF
Other networks	Any IP network available to the machine
Network hardware	Consumer networks and consumer network hardware; no proprietary hardware or custom cellular links
Typical deployment	2 or 3 network interfaces bonded into one logical link

AGGREGATION AND SCHEDULING

Aggregation mode	Active-active: all links carry traffic at the same time, with no failover switchover time
Tradeoff control	Configurable per traffic class across latency, reliability, and bandwidth; common settings are minimize latency and maximize bandwidth
Data sharding	Erasur coding in two dimensions: parallel packets on independent interfaces and sequential packets on one interface
Packet handling	Intelligent packing and fragmentation; MTU-aware and tunnel-priority-aware
Traffic classes	Multiple tunnels per connection, scheduled cooperatively; lower-priority data waits for higher-priority data

LINK MONITORING

Link state events	Automatic detection of link up and down events and new routes on each interface
Bandwidth estimation	Continuous online estimate of the bottleneck bandwidth rate (BBR) of each link
Exogenous signals	Wireless signal conditions (RSSI, SNR, code allocations), retry rate, GPS location
Predictive scheduling	Avoids links that are degrading, and can down-weight carriers in locations where they are known to struggle

NETWORKING AND SECURITY

Topology	Point-to-point tunnels (not a VPN), with lower encapsulation overhead and lower latency than VPN-based bonding
Endpoints	Two per connection: one software instance on each peer
NAT traversal	Bi-directional connectivity between hosts behind NAT or CGNAT, with no router or firewall configuration on either side
Peer discovery	Automatic; peers identify by public key, with no static network configuration. After a session starts, peers discover non-publicly routable links directly and no longer depend on the discovery service
Encryption	End-to-end encryption of all traffic; endpoints verify each other with asymmetric cryptography; key management handled automatically

METRICS AND DIAGNOSTICS

Link metrics	Network characteristics and link aliveness for every link
Tunnel logs	Detailed logs for every tunnel to reconstruct and root-cause incidents
Tools	Validate, investigate, and tune tunnel behavior for any objective

DEPLOYMENT

Delivery	Software
Host hardware	Runs on your own hardware
Supported operating systems	Contact FORT Robotics for current platform support
Integration	Integration support from FORT Robotics is available for your deployment
Availability	Q4 2026

04**Ordering Information****PART NUMBER DESCRIPTION**

FSW-ESS-CONNAGG	Connectivity Aggregation software
-----------------	-----------------------------------

For pricing and additional information, contact your FORT Account Executive or sales@fortrobotics.com.

05

Related Documentation

- FORT product documentation: fortrobotics.com/docs

Specifications are subject to change without notice. For the most current information, visit fortrobotics.com/docs.

© 2026 FORT Robotics, Inc. All rights reserved. FORT, FORT Robotics, and the FORT logo are trademarks of FORT Robotics, Inc. All other trademarks are the property of their respective owners.