centiel

SWISS MADE

Vietnam Telecom Power Resilience Guide

DARA TECH

Green UPS

How Distributed UPS Architecture Reduces Fleet-Wide Risk During Network Expansion

A technical guide for telecom infrastructure and power engineering teams managing multi-site UPS fleets across Vietnam

Article

By **Gerardo Lecuona**
Co-founder & Global Sales Director
CENTIEL SA

centiel.com

Three Scenarios. One Root Cause.

Vietnam's telecom operators are expanding rapidly — new towers, edge nodes, regional NOCs, and transmission hubs. Each new site brings a UPS. But the architecture that gets replicated across that fleet rarely changes. The scenarios below are not hypothetical.

Bypass during routine maintenance. A regional hub site enters bypass during a scheduled PM window. Three downstream dependent services lose protection. The event was foreseeable — it was structural, not accidental.

Controller fault replicated at scale. A controller anomaly triggers a full-system bypass transfer. The same failure pattern has already appeared at three other sites running identical UPS topology. Same design, same exposure.

Expansion blocked by architecture risk. Network expansion is approved and budget is available. But operations cannot commit to rollout because every new site will replicate the same architecture risk. Growth stalls.

> ***These are not isolated incidents.*** *They are symptoms of centralised power dependency repeated across a growing portfolio. The failure mode is not unique to one vendor, one site, or one event. It is the architecture.*

This guide explains what that architecture looks like, why it compounds at fleet scale, and how a distributed design approach changes the risk profile. It covers how **availability** is calculated, what the difference between six-nines and nine-nines means for your **SLA exposure**, and how to evaluate **redundancy** architecture before you specify.

The technical content draws on Centiel's **DARA** (Distributed Active Redundant Architecture), which underpins the CumulusPower & StratusPower fourth-generation modular UPS. The evaluation framework in Section 5 applies regardless of vendor.

The Number Behind Availability at Fleet Scale

A single site with a 99.9% available UPS system experiences roughly 8.7 hours of unplanned exposure per year. That is an acceptable individual risk for many operations. But telecom networks do not run on individual sites — they run on fleets. And at fleet scale, availability mathematics compound.

The question is not whether one site will have an event. It is how often somewhere in your fleet will.

Availability is typically expressed as a number of nines. Most third-generation modular UPS architectures deliver **six nines** (99.9999%). Centiel's StratusPower & CumulusPower, through **DARA**, delivers **nine nines** (99.9999999%).

A single UPS architecture choice is a local decision. Replicate it across 50, 100, or 200 sites and it becomes a fleet-wide policy. The availability mathematics do not add — they multiply.

$$A = \frac{MTBF}{MTBF + MTTR}$$

Fleet Availability = A^n (*n sites, independent*)

The Number Behind Availability at Fleet Scale

Architecture Risk Profile	1 Site	50 Sites	200 Sites
Shared bypass exposure event	Rare — once in several years	Realistic — several per year	Frequent — multiple per quarter
Controller-triggered full transfer	Low probability	Measurable fleet event	Likely recurring issue
Maintenance-induced exposure window	Controlled, one site	Concurrent windows across region	Concurrent windows, multiple regions
Architecture flaw replicated to new site	Single incident	System-wide pattern	National fleet vulnerability

> ***At telecom scale, probability compounds faster than budgets.*** *The architecture you specify today is the fleet risk you manage in five years.*

Why Telecom Networks Already Understand This

Telecom engineers understand distributed resilience deeply. It is the design principle behind every core network you operate.

Design Decision	Your Network Architecture	Conventional UPS Architecture
Routing	Multiple independent paths. No single route dependency.	Single bypass path shared by all modules. One path, one failure point.
Control Logic	Distributed routing decisions. No single controller bottleneck.	Central controller decides for all modules. One fault, full-system response.
Redundancy model	Active-active. All nodes carry load. No cold standby.	Passive standby in many designs. Standby module not load-tested until needed.
Failure domain	A node failure stays local. Traffic reroutes. Service continues.	A module fault can trigger full bypass. All load loses protection.
Maintenance model	Nodes maintained live. Traffic reroutes. No service window.	Maintenance often requires bypass transfer. Exposure is planned, not eliminated.

The question is not whether distributed resilience works. You already operate it every day across your network. **The question is why the power infrastructure protecting that network is still built on the centralized dependency model your network architects replaced twenty years ago.**

> Your network avoids single routes. Single routers. Single controllers. Single peering dependencies.
>
> **So why accept shared UPS control logic? Common bypass dependency? Centralized transfer decisions?**
>
> **DARA** applies the same design logic your network already uses — to the power layer that keeps it running.

Distributed. Active. Redundant.

DARA stands for Distributed Active Redundant Architecture. It is the design principle underlying Centiel's StratusPower & CumulusPower fourth-generation modular UPS system. Each word describes a specific architectural property — and each property directly affects the **availability** calculation.

Distributed

Distributed means that a decentralised architecture is used. No single active component can be a potential **single point of failure**. No single control board, no single static bypass, no single parallel bus. Each module within the frame is a fully independent UPS with self-isolating **Intelligent Module Technology (IMT)**, containing all the building blocks of a complete UPS unit: rectifier, inverter, static bypass, battery charger, control logic, and control panel.

The practical consequence for a **telecom network**: a fault in one module stays in one module. It does not cascade to the system. It does not disrupt protection at adjacent sites sharing the same rollout architecture. The failure domain is contained by design.

Lesser quality modular UPS units use a single separate static bypass, which becomes a potential **single point of failure**.

Active

DARA's Distributed Decision Making (**DDM**) technology means there is no single component deciding for the complete UPS system. Instead, **the sum of the modules' decisions determines the total system action** in response to any issue.

In typical modular UPS architecture, a single decision-making point has a problem — it signals the entire system to transfer the load to static bypass. Centiel's true modular UPS with **DARA** makes distributed decisions.

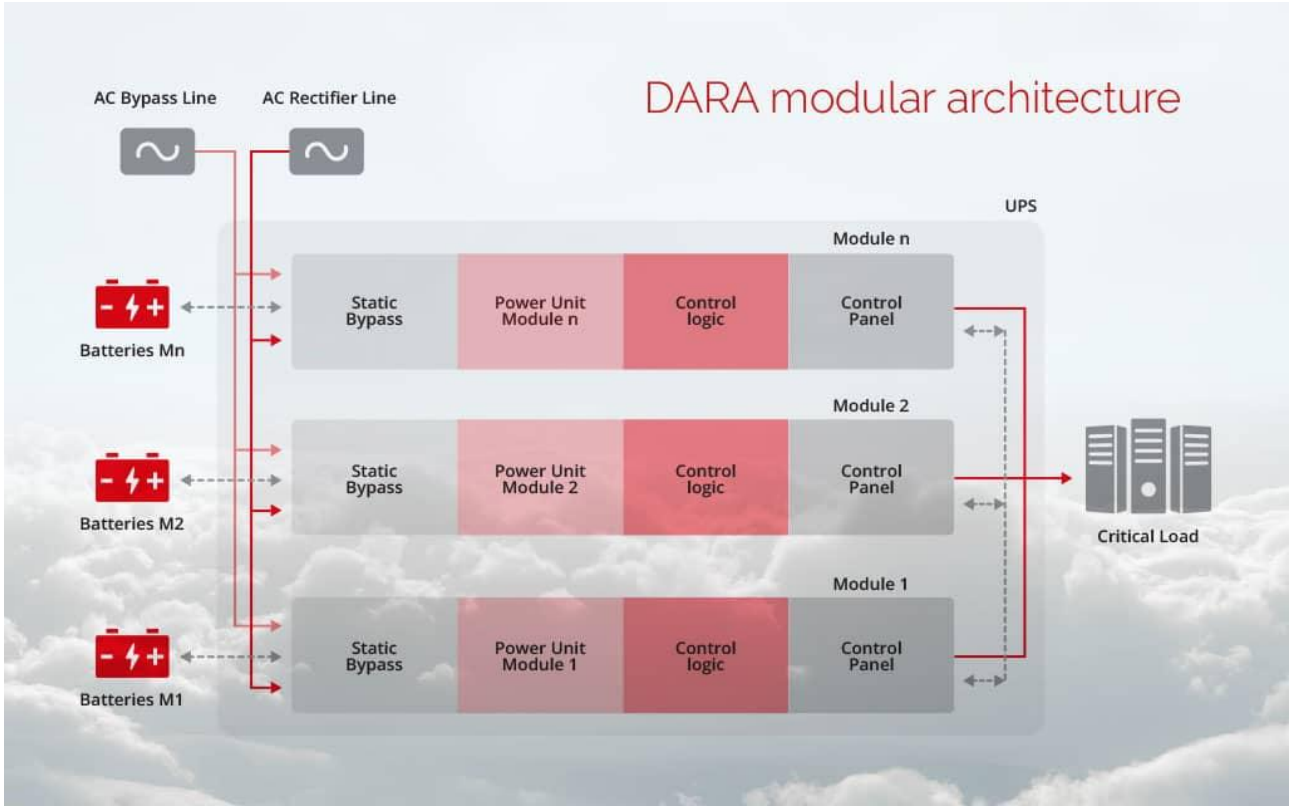
At module level, if a fault occurs, that module communicates instantaneously with all remaining modules via a **Triple Mode parallel BUS** — three independent, triple-**redundant** communication paths. The affected module and the system respond together. The critical load remains protected throughout. A controller anomaly at one site does not replicate itself across every site running the same topology.

Redundant

Redundancy in a **DARA** system operates at the module level. Adding modules above the number required creates N+1 or higher redundancy — each additional module is an active, load-sharing participant, not a passive standby.

This has a direct consequence for **maintenance in distributed telecom environments**: any single module can be isolated, removed, and replaced while the system continues to support the full load on remaining modules. No maintenance window. No transfer to bypass. No planned exposure event — at that site or any other running concurrently.

Centiel's **safe hot-swap** capability extends this further. A replacement module introduced to a live system is fully isolated and tested within the running frame before it accepts any load. Any fault in the replacement module is identified before integration — eliminating the risk of a faulty module causing a **cascading fault** in a live network.



Where Centralized Architectures Break at Scale

Centralized architecture failures are not random events. They are predictable consequences of specific design choices. When those choices are replicated across a growing fleet, the consequences scale proportionally.

Failure Mode	Centralized Architecture	DARA Architecture
Shared Controller	One logic fault signals the entire system. All modules respond identically. Full transfer to bypass. All load exposed.	No single controller. Each module uses DDM to make distributed decisions. A fault in one module does not command the rest.
Shared Bypass Logic	A local event becomes a facility event. One bypass, all load. One fault, one protection window for everything.	Each module contains its own static bypass. A bypass event in one module stays in that module. Adjacent load remains protected.
Maintenance Dependency	Routine preventive maintenance requires bypass transfer at the system level. Every PM visit is a planned risk event.	Modules are maintained live. Any single module is isolated and replaced while the system runs at full load on remaining modules.
Copy-Paste Architecture	Specification file from Site 1 becomes spec for Sites 2–200. One architectural weakness becomes a national fleet vulnerability.	A standardized modular architecture scales resiliently. Each site inherits the same distributed failure containment by default.
Safe Hot-Swap	A replacement module introduced to a live system is not tested before it accepts load. A faulty module can cause a cascading event.	DARA's safe hot-swap capability fully isolates and tests a replacement module within the running frame before it accepts any load.

The Vietnam UPS market analysis (2025) notes that channel partners rarely publish deep coverage of Tier III/IV architecture, PUE optimization, or AI-class power design. **This is the gap. Operators who understand the architecture difference make better fleet decisions. Those who do not replicate the weakness.**

The Maintenance Window Is a Vietnam Telecom Problem

Vietnam's telecom infrastructure expansion is pushing sites into environments where **conventional maintenance models create real operational risk**. The combination of remote locations, technician availability, and local climate conditions makes **planned exposure windows a serious concern** — not a theoretical one.

Operational Factor	Conventional UPS Impact	DARA Impact
Remote tower sites	Maintenance requires travel to site. Bypass event scheduled around travel window, not operational risk.	Module replacement can be performed by a local technician with standard tools. No bypass required.
Technician scarcity	Specialist UPS engineers are in short supply across provincial markets. Response time measured in days.	Low MTTR by design. Standard technicians can replace modules safely. Specialist availability is not a dependency.
Hot and humid climate	Accelerated battery and fan degradation. Replacement frequency increases. Each replacement in a conventional system is a bypass event.	Battery modules and fans are hot-swappable at module level. Climate-driven replacement cycles do not increase system-level exposure.
Battery replacement cycles	Battery replacement in a centralized architecture requires system-level coordination. Often deferred until failure.	Modular battery replacement is performed per module, live, without transfer. Proactive replacement becomes operationally straightforward.
Fleet PM scheduling	PM visits create recurring bypass events across the fleet. PM calendar is a risk calendar.	PM is performed live. No bypass events. PM calendar does not generate SLA exposure.

Architecture should reduce field dependency, not increase it.

Every maintenance event in a conventional UPS design is a planned exposure event. **DARA eliminates the category.**

Five Questions for Any UPS Vendor

The following questions apply to any UPS vendor evaluation — new installation, capacity expansion, or replacement of end-of-life equipment. They are designed to surface the architectural properties that determine real-world **availability** in a **telecom fleet** context.

1 Does each module contain its own static bypass, or is bypass centralised?

*A centralised static bypass is a **single point of failure**. Ask for a circuit diagram, not a marketing description.*

2 Can a replacement module be isolated and tested within a live frame before it accepts load?

*This is the distinction between **hot-swap** and **safe hot-swap**. If the answer is no, the maintenance procedure relies on the replacement module being fault-free at insertion — a procedural assumption, not an architectural guarantee.*

3 What is your documented **MTTR** for a **module replacement** under live operational conditions, and does your **SLA** carry financial penalties for breach?

*A vendor who cannot answer the first part has not measured it. A vendor who cannot answer the second is offering **availability** assurance without commercial accountability.*

4 How does your control logic respond to a module-level fault — distributed decision-making or centralised transfer to bypass?

Ask specifically what happens to the load on all other modules when a single module faults. Centralised = system-wide response. Distributed = fault stays local.

5 What is your published **availability** figure, how is it calculated, and what is the **MTBF** at full rated load?

*Nine nines, **six nines**, and **five nines** are not equivalent. Require the calculation methodology, not just the headline figure.*

> *These questions will not be comfortable for vendors whose architecture relies on centralised components. They are the right questions regardless.*

In Practice

Redcentric | UK | Managed IT & Colocation | StratusPower — 14 × 500kW Modular UPS Systems

Redcentric is a leading UK **managed IT** and **colocation** provider operating the Heathrow Corporate Park data centre in London. In 2023, Redcentric undertook a full electrical infrastructure upgrade including the live replacement of legacy UPS systems before end of life. Centiel supplied StratusPower modular UPS equipment to protect an existing 7 MW critical load.

Outcome:

- Upgrade completed with **zero downtime** or disruption
- UPS operating efficiency rose from below 90% to **more than 97%**
- System design enables capacity increase to 10.5 MW without additional infrastructure
- Potential to reduce more than 8,000 tonnes of CO_2 emissions over 15 years
- 2026: further 12 MW deployment planned for two halls being configured for AI workloads
-

"With no commissioning issues and zero reliability challenges or problems with the product, we are already talking to the Centiel team about how they can potentially support us with power protection at our other sites."

— Paul Hone, Data Centre Facilities Director, Redcentric

Taiwan Power Company (Taipower) | Taiwan | Public Services / Data Centre | Three-phase modular UPS

Taiwan Power Company (Taipower) is Taiwan's state-owned electric power utility. It required a reliable, robust, and future-proof power protection system for its new Central Data Centre in Changhua — a facility essential for government initiatives involving big data, AI, and cloud computing.

Relevance for Vietnam telecom operators:

- Procurement through formal government process — demonstrates suitability for regulated and state-linked operators
- Regional proximity and cultural alignment with Vietnam's critical infrastructure environment

- Deployment to tight project schedule — relevant for phased network rollout programs
- AI and cloud readiness — aligned with Vietnam's digital infrastructure growth trajectory

"Centiel's expertise in delivering reliable power solutions confirms its position as a trusted partner for critical projects globally."
— Taiwan Power Company Case Study, Centiel SA

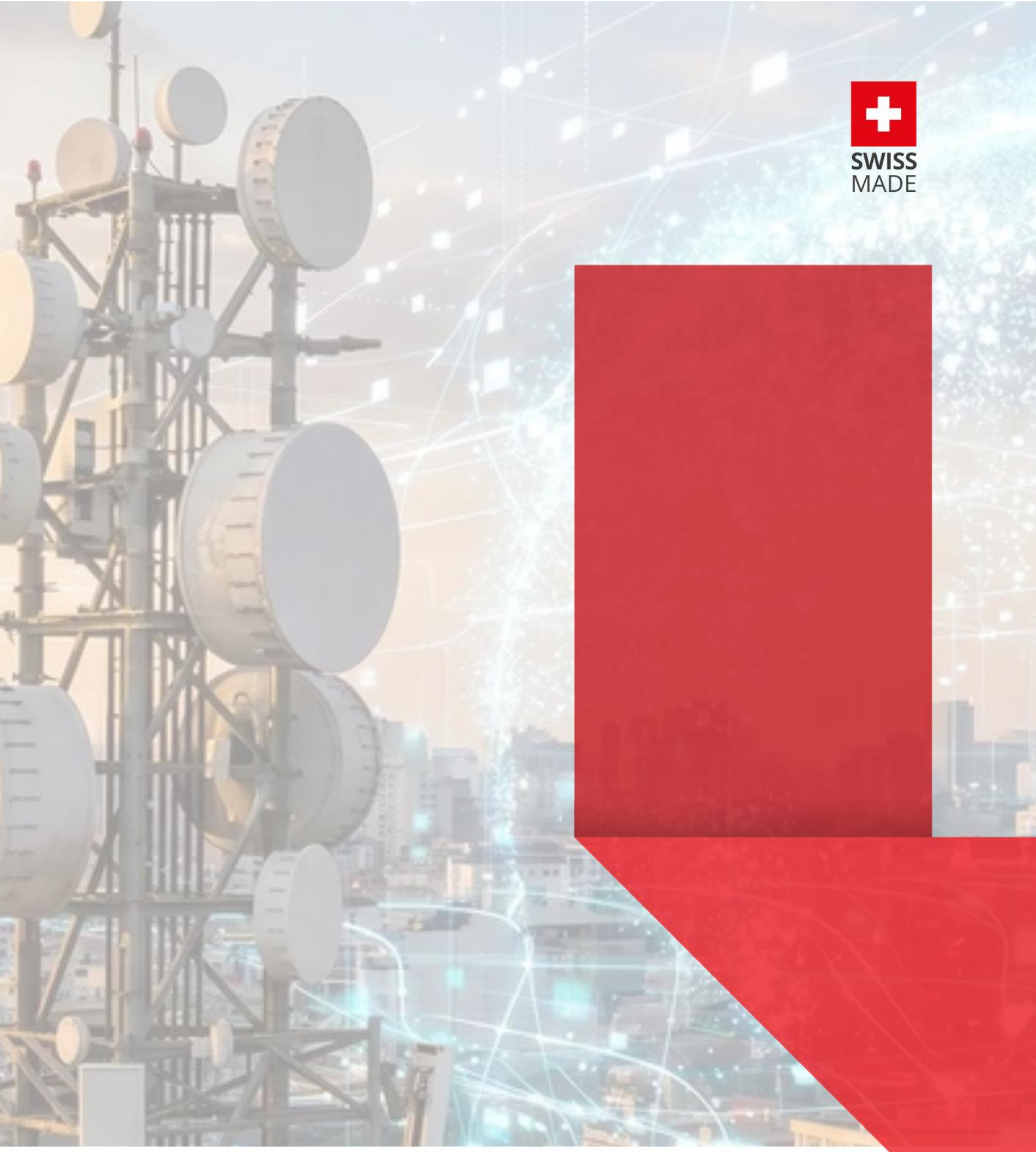
StratusPower & CumulusPower are installed and operational in critical facilities across more than 60 countries on five continents.

Book a Telecom Architecture Review

A structured technical conversation covering your current power architecture, redundancy configuration, and fleet-scale risk exposure. The right next step if you are evaluating a UPS specification for multi-site rollout, replacing legacy equipment in live facilities, or preparing for 5G, edge, or AI-workload density increases.

Request a 30-minute technical review with a Centiel engineer here.

centiel.com | Swiss Made



SWISS
MADE

centiel
continuous power availability

centiel.com