



## Case study

# Data center-grade IT protection on the aerospace factory floor: securing critical infrastructure in additive manufacturing environments



## Background

Additive manufacturing (3D printing) is now essential to aerospace production by enabling high-precision, lightweight components that meet strict industry standards. These systems depend on dedicated IT infrastructure such as servers, networking, and storage to manage real-time control, quality monitoring, and production data.

The reliability of this IT infrastructure directly determines production continuity, as aerospace production environments are inherently hostile to sensitive IT equipment. Manufacturing floors expose computing systems to metallic dust, temperature fluctuations, and humidity, all conditions that significantly reduce equipment lifespan and increase failure risk.

The traditional solution, building dedicated, climate-controlled server rooms, introduces higher costs, longer project timelines, and physical separation from the production process.



## Challenge

A global aerospace manufacturer operating advanced additive manufacturing systems faced a critical infrastructure reliability issue. The servers controlling the 3D printing processes were installed directly in the production area to provide low-latency connectivity with manufacturing equipment.

This setup exposed the IT infrastructure to several operational challenges:

- Airborne contamination: High concentrations of fine metallic dust infiltrated server ventilation systems, gradually clogging filters and heat sinks.
- Thermal instability: The production floor lacked dedicated climate control for IT equipment, leading to temperature fluctuations beyond recommended operating ranges.

- Continuous operation requirements: Aerospace manufacturing runs on tight schedules with minimal tolerance for downtime. Any IT failure immediately stopped production lines, impacting delivery.
- Accelerated hardware degradation: The combination impact of dust and thermal stress aged the equipment prematurely, and increased failure frequency.

As a result, the customer experienced recurring server failures and unplanned maintenance. Each failure triggered production interruptions, emergency corrective actions, lost production hours, increased maintenance costs, and risk to quality standards. Without a purpose-built environmental protection solution, the IT infrastructure remained a critical vulnerability within an otherwise highly controlled manufacturing process.



## Solution

To address these challenges, the aerospace manufacturer deployed the Vertiv™ SmartCabinet™ ID, a fully enclosed, environmentally protected micro data center installed directly within the production area, close to the systems supporting critical 3D printing operations.

Rather than addressing a high heat-density application not required, the primary objective was to create a clean, controlled, and highly reliable IT environment capable of protecting sensitive servers from industrial contaminants. In the manufacturing area, airborne dust, metallic particles, and humidity fluctuations were compromising server performance and increasing the risk of unplanned downtime.

The Vertiv™ SmartCabinet™ ID features an IP54-rated enclosure that physically isolates IT equipment from dust, debris, and moisture, providing a protected environment that helps servers operate under optimal conditions. By preventing contaminants from reaching critical components, the solution improves system reliability and reduces the risk of failures associated with industrial environments.

Its integrated thermal management system is designed to maintain stable environmental conditions inside the cabinet, automatically adapting to IT load requirements and supporting consistent server performance regardless of variations in the surrounding production environment. An external heat rejection unit enables flexible deployment while maintaining reliable operation across a wide range of ambient temperatures.

Additionally, the built-in 9-inch HMI touchscreen provides centralized monitoring and control of key operational parameters, including temperature, humidity, power status, alarms, and security functions.

Instead of investing in the construction of a dedicated IT room with separate HVAC, power, and security infrastructure, the Vertiv SmartCabinet ID was deployed in just a few days. The pre-engineered, factory-integrated architecture arrives ready for installation, significantly accelerating implementation while reducing project complexity.

To further enhance power availability and infrastructure visibility, the solution was complemented by Vertiv™ Liebert® GXT5 UPS systems for continuous power protection and Vertiv™ PowerIT rPDUs for advanced power distribution monitoring and management.





## Results

By deploying the Vertiv™ SmartCabinet™ ID, the aerospace manufacturer achieved:

- A protected IT environment that shields mission-critical servers from industrial dust, metallic particles, and other contaminants.
- Optimized operating conditions for servers, supporting consistent performance and reliability.
- Reduced equipment failures associated with contamination and environmental exposure.
- Improved production continuity through the increased reliability of the IT systems supporting 3D printing operations.
- Lower maintenance requirements and reduced downtime, minimizing interventions and improving system availability.

- Rapid deployment of edge infrastructure directly alongside manufacturing equipment without the need for a dedicated server room.
- Scalable and future-ready architecture capable of supporting evolving production and computing requirements.
- Enhanced operational resilience, supporting the continuous availability of critical manufacturing processes.

This deployment demonstrates how protecting IT infrastructure from environmental contamination can be as important as thermal management in industrial edge environments, enabling reliable server operation directly on the factory floor while supporting business-critical manufacturing processes.

“In aerospace manufacturing, IT infrastructure is no longer a back-office function, it is embedded at the heart of the production process. When servers control additive manufacturing systems producing flight-critical components, any IT failure becomes a production failure. The Vertiv™ SmartCabinet™ ID brings data center-grade environmental protection directly to the factory floor, enabling aerospace manufacturers to deploy critical IT exactly where it is needed, while supporting reliability, avoiding the need for dedicated rooms, and reducing the delays associated with traditional construction.”

— **Giuseppe Leto**

*Senior Director IT Systems Business EMEA, Vertiv*