

Security by Design for Space: How Celeste Technologies Secured Its 5G Satellite RAN



Executive Summary

Celeste Technologies is developing SmartgNB, a software-defined gNB for Non-Terrestrial Networks (NTN), extending 5G communications into space. Before market deployment, Celeste collaborated with HWG Sababa on advanced product security testing combining secure code review, threat modeling, and fuzz testing.

The project identified and prioritized resolution to security weaknesses, improved software resilience, and helped embed secure development practices into future product releases – strengthening Celeste's secure-by-design approach before commercial launch and supporting its readiness for future operator and institutional engagements.

Key Results

- 20+ security findings identified and addressed before commercial launch
- 8 findings validated as exploitable in a running environment and remediated prior to deployment
- Improved resilience of the system through advanced security validation and testing
- Secure development practices integrated into the engineering process
- Foundation established for continuous fuzz testing and future security assessments
- Increased readiness for deployment in critical communications environments

Company Background

To reach beyond traditional terrestrial boundaries and unlock new use cases, telecommunications standards are actively incorporating satellite communications into the 5G ecosystem. By bringing satellite networks directly into 3GPP specifications, the industry is creating a unified framework designed to deliver resilient connectivity to remote and mission-critical regions, complementing existing Terrestrial Networks infrastructure.

To power this expansion, Celeste Technologies, an Italian deep-tech company, develops fully software-defined 5G infrastructure tailored for spaceborne networks. Its flagship solution, SmartgNB, is a virtualized 5G base station (gNodeB) software stack designed to extend standard, 3GPP-compliant mobile communications into satellite environments.

Unlike traditional telecom infrastructures that rely on tightly integrated hardware and software platforms, Celeste's software-defined approach enables greater flexibility, scalability, and interoperability across next-generation satellite networks.

Operating at the intersection of telecommunications and space technologies, the company is helping shape a new generation of satellite connectivity services while addressing the unique technical challenges of deploying critical communications infrastructure in space.

Key Challenges

For Celeste Technologies, the challenge was not simply developing a new telecommunications solution. It was demonstrating that a young company operating in an emerging market could deliver technology aligned with the expectations of future operators, institutional stakeholders, and critical communications environments.

Because the platform is intended for satellite-based infrastructure, security, resilience, and reliability had to be considered from the beginning of development rather than addressed later through compliance initiatives or customer requests.

Security in a Space Environment. Systems deployed on satellites cannot be physically accessed or repaired, requiring high levels of reliability and resilience from the outset.

Real-Time Performance Constraints. The platform operates in a real-time environment with strict latency requirements, limiting the ability to introduce heavy security controls without affecting performance.

Complex, Multi-Interface Architecture. Multiple communication and control interfaces expand the potential attack surface and require careful security validation.

Balancing Innovation and Security. As a fast-growing company with strong R&D capabilities, Celeste needed to align rapid development cycles with secure coding practices and long-term product robustness.

“We knew from the beginning that cybersecurity had to be a priority. We are developing critical telecommunications infrastructure, and we wanted security to be part of the product roadmap from the outset – rather than retrofitted in response to market demand.”

– Fabio Marconi, Co-Founder and Product Manager at Celeste Technologies

The Solution: Product Security Assessment and Penetration Testing

To address these challenges, Celeste Technologies collaborated with HWG Sababa to conduct advanced penetration testing of its software-defined 5G NTN gNB. The engagement focused on validating the security and resilience of a highly complex codebase comprising millions of lines of code and implementing advanced telecommunications protocols based on international 3GPP standards.

To provide both architectural and implementation-level assurance, the assessment combined three complementary activities:

Secure Code Review

A detailed review of the platform's source code identified vulnerabilities, insecure coding patterns, and opportunities to strengthen software resilience while preserving performance requirements.

Threat Modeling

The system architecture and interfaces were analyzed to identify potential attack vectors, evaluate exposure points, and prioritize mitigation efforts.

Fuzz Testing

A dedicated testing environment was created to evaluate how the platform responded to unexpected or malformed inputs, helping uncover weaknesses that could affect stability, reliability, or security.

Scope of Testing

- Secure code analysis and vulnerability identification
- Architecture-level threat modeling
- Simulation-based testing environment
- Advanced fuzz testing for resilience validation
- Actionable remediation guidance for future development

“It was truly a collaborative effort. HWG Sababa quickly grasped the key aspects of our technology, providing actionable insights, analyses and recommendations that immediately strengthened both our product and our development processes.”

– Vincenzo Icolari, Head of Research & Development at Celeste Technologies

Results and Business Impact

The engagement delivered immediate security improvements while helping Celeste strengthen its long-term product development strategy, reduce risk before commercial deployment, and increase readiness for future market opportunities.

Security Improvements

The assessment identified more than 20 security areas of improvement across the platform, including 8 vulnerabilities validated as exploitable in a running environment. These findings provided Celeste with a prioritized remediation roadmap, enabling the engineering team to address critical risks early in the product lifecycle and further strengthen the security of its software-defined NTN gNB.

Stronger Development Practices

The findings and recommendations helped Celeste refine its engineering approach and reinforce secure coding principles across the development lifecycle. Security testing became more closely integrated into product development activities, reducing the likelihood of recurring issues in future releases.

Internal Capability Building

In addition to identifying vulnerabilities, HWG Sababa provided methodologies, testing approaches, and practical guidance that can be incorporated into Celeste's internal validation processes. This knowledge transfer helped establish a foundation for continuous security testing as the platform continues to evolve.

Strategic Readiness

By addressing security early in the product lifecycle, Celeste strengthened its ability to demonstrate a proactive and mature approach to cybersecurity. The project enhanced the company's readiness for future engagements with telecommunications operators, institutional organizations, and other stakeholders operating in critical communications environments, where security and resilience are key evaluation criteria.

The engagement also helped Celeste demonstrate that cybersecurity is embedded into the product development process – an important factor in building trust with future customers, operators, and ecosystem partners.

As the platform continues to evolve, Celeste is evaluating the implementation of continuous fuzz testing capabilities and additional security validation activities to support product resilience, scalability, and deployment readiness.

"The value extended beyond simply identifying and resolving vulnerabilities. We strengthened our development process, equipping our team with tools and methodologies that scale as the product evolves. We didn't just receive a checklist of fixes – we have improved our cybersecurity practices and built them into our engineering culture and long-term product roadmap."

– Chiara Grasselli, Cybersecurity Expert at Celeste Technologies