Global Navigation Satellite Systems (GNSS) is nowadays used as a timing source for the synchronization of various types of networks. It has been recently defined as "the backbone of the connected world" or "the invisible utility" to highlight its pervasive presence in our daily life. Some of these networks are classified as critical infrastructures and, together with other service infrastructures, pose security-related requirements on top of timing accuracy requirements. Through Horizon 2020, the European Union's programme for research and innovation, the EUSPA selected the ROOT project to demonstrate the benefit of Galileo OSNMA signal to increase the robustness of critical telecom infrastructures (under the topic 'EGNSS applications fostering societal resilience and protecting the environment').

For many years Septentrio has been active in European projects focusing on developing state-of-the-art GNSS (Global Navigation Satellite Systems) technologies and products. Today, the company is established as a key player on the European GNSS market. For ROOT, Septentrio has been teaming up with experts all around Europe to focus specifically on challenges for the telecommunication market. ROOT partners cover the whole value chain for critical infrastructures: from research to manufacturers of GNSS and timing components, from networks operators to experts in market strategies. These partners complement each other in terms of knowledge and competences.

Long-term stability and accurate time synchronization are at the core of timing network facilities in critical infrastructure, such as telecommunication networks. In these applications, timing signals output by GNSS receivers, i.e., One Pulse-per-Second (1-PPS), complement Primary Reference Time Clocks (PRTCs) by compensating for long-term drifts of their embedded atomic clocks. However, GNSS receivers may expose timing distribution networks to Radio Frequency (RF) vulnerabilities, causing degraded or disrupted synchronization of the nodes. Despite the growing dependency on GNSS, network operators rarely perceive the vulnerability of GNSS receivers to spoofing or jamming as a real problem. The awareness about GNSS spoofing, namely the transmission of false signals remains very low in the industry. During a spoofing attack, a nearby radio transmitter sends fake GNSS signals to the target receiver, fooling it into believing it is at a false location and compromised timing. By the time signals from GNSS satellites reach the Earth they are very weak and can easily be overpowered by signals in the same frequency range transmitted from nearby. A spoofer can gain control of a target GPS receiver, taking over navigation and timing functionality of the whole system. For applications such as critical infrastructure, this is a serious vulnerability.

ROOT stands for *Rolling Out OSNMA for the secure synchronization of Telecom networks* and the project aims to experimentally demonstrate the benefits introduced by new multi-frequency GNSS timing receivers, which are able to process the Galileo OSNMA signals. OSNAM (Open Service Navigation Message Authentication) signals use cryptography, meaning

that satellite signals can be authenticated or verified by the user. Only those signals which pass the authentication test are used in the positioning and timing algorithms. The European Galileo GNSS constellation is pioneering signal authentication with OSNMA , which is now in test phase. Running cryptography algorithms on embedded devices is computation intensive and requires powerful processing capabilities available in Septentrio products. If a satellite signal is flagged as spoofed, it is excluded from the timing calculation.

During the ROOT project, Septentrio released the new mosaic-T GNSS receiver dedicated to time synchronization applications. Along with resilient network synchronization architectures for long-distance accurate time distribution, ROOT proved that it is possible to improve the current resilience of telecom networks, matching the requirements posed by future 5G systems. Following an experimental approach, the project demonstrated new strategies for secure network synchronization, which combine GNSS signal authentication, interference monitoring algorithms, autonomous switching between timing sources, remote attestation of software to protect from cyberattacks.

An important part of the project was also to increase the market awareness of the problem of intentional Radio Frequency Interference (RFI) and cyber-attacks against GNSS timing receivers. Through a permanent presence on social networks, several technical papers presented in conferences, as well as a short video published on the ROOT project website https://www.gnss-root.eu/ we can say that the ROOT project reached that target. The presentation of the ROOT architecture to management teams of some major Telecom operators in Europe also contributes to a more resilient European infrastructure in the future.

The ROOT project started back in November 2020, right before the start of the Covid-19 pandemic. It ended some months ago with a very positive evaluation from the European Agency for the Space Program. Despite a very difficult time that prevented physical interaction between teams across Europe, the partners managed to successfully complete this project. Moreover, the experimental phase of the ROOT project overlapped with the Galileo OSNMA public testing phase and the partners could go beyond the original project scope, carrying out tests on live OSNMA signals. At Septentrio, we are very proud of the work done by our team in such very difficult times. The results of the project partially close a gap in the security of telecommunication networks dependent on satellite-derived time, with indirect benefits in curbing illegal attempts to disrupt network services.