

Regulus is the first company dealing with sensor security, enabling uninterrupted, continuous operation under malicious attacks or accidental interference to sensors.

From GNSS (Global Navigation Satellite System) to LiDAR and Radar, sensors are critical components across a wide range of applications: vehicles on the ground, in the air and at sea; and critical infrastructure (telecom, power grids, financial institutes). Today, little is done to secure sensors against spoofing and jamming attacks. The sensor threat is growing rapidly with real-world attacks happening across these multiple sectors and is expected to further grow as sensor-dependent systems become more connected and autonomous.

To face these threats, Regulus is developing Pyramid – a set of technologies aimed at solving this problem.

Pyramid GNSS

The Pyramid GNSS technology is a breakthrough in the ability to create GNSS receivers that are protected against spoofing and jamming attacks. It allows detection, mitigation and reporting of both spoofing and jamming attacks while still providing accurate position, navigation and timing. It is the first solution relevant to the commercial sector in terms of performance, price, size and weight.

Spoofing is a smart attack on GNSS receivers, allowing an attacker to pose as a legitimate satellite signal, enabling him to manipulate and deceive the receiver, causing severe unexpected behavior.

Jamming is a denial of service attack, causing the GNSS receiver to fail in providing a PNT solution due to high levels of noise created by the jammer.

The GNSS Opportunity

GNSS plays a critical role in next-generation positioning and timing systems as the only source of absolute position, velocity and time. The GNSS industry's global revenue is currently over \$85B and is expected to grow beyond \$100B in 2021 with 22 billion devices globally, according to the European Global Navigation Satellite Systems Agency (GSA). At the same time, the LBS (Location Based Services) market is expected to reach \$250B in 2021.

Pyramid LiDAR

LiDAR is prone to different spoofing and jamming attacks. Since the sensor has to perform very complex tasks, while becoming smaller and more affordable, security at the sensor level is challenging to implement. Pyramid LiDAR is an independent, external solution, detecting attacks against the LiDAR suite. The Pyramid LiDAR, now in early research, is the only dedicated system looking at LiDAR security today and is also designed with commercial use cases in mind.

About Regulus Cyber

Regulus is engaged with major companies and organizations - OEMs, Tier 1, high-tech companies and government agencies in the automotive, aviation and telecom industries. Currently, technical pilots are being offered towards commercialization of the full Pyramid technology in 2019. Successful pilots and collaborations have been arranged with AT&T, NASA (in partnership with North Dakota's NP UAS test site), Swiss Drones, and leading companies worldwide.

Regulus was incorporated in December, 2016, and in 2017 raised \$6.3M in seed and series A funding from leading investors - Sierra Ventures, Canaan Partners Israel, The Technion University ("Israel's MIT") and F2 Capital. Regulus is an alumnus of the prestigious "The Junction" accelerator in Israel.

The Regulus Pyramid won first prize for Cyber Security at the most important expo for unmanned systems – the AUVSI EXPONENTIAL 2018.

Regulus was founded by technical and operational veterans of the Israeli Airforce, 8200 (the Israeli Army's elite intelligence unit), Elbit Systems, Rafael and Israel Aerospace Industries, with years of experience in sensors, data links, encryption and unmanned systems.