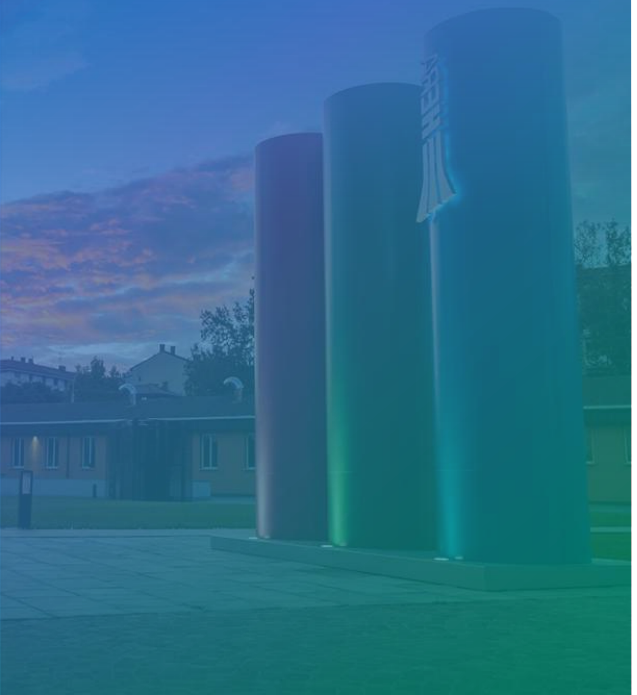
Cybersecurity of Infrastructures in Hera Group

Solid infrastructures for a long-term sustainable strategy

Photo by Silvia Camporesi: construction phase of the biomethane plant of Sant'Agata Bolognese

Protection of infrastructures



Protecting infrastructures is an absolute priority for Hera, especially in a context where cyber threats are constantly evolving and becoming increasingly sophisticated. To ensure the resilience and security of its essential services, Hera has developed and implemented a series of dedicated programmes and initiatives focused on cybersecurity, with particular attention to operational technologies (OT).

Cyber Risk Management in Operational Technologies
Hera adopts a structured approach to cyber risk management, with specific initiatives aimed at operational technologies and industrial systems. Through the identification, assessment, and monitoring of risks associated with OT environments, the company implements preventive and corrective measures to reduce the attack surface and strengthen the security of its critical assets. International standards and sector best practices are also adopted to ensure maximum protection of both physical infrastructure and digital systems.

Collaboration and Information Sharing with Government Agencies
Aware of the importance of cooperation in countering cyber threats, Hera actively participates in working groups and joint initiatives with leading government agencies and authorities responsible for national and cyber security. The company actively collaborates with the Agenzia per la Cybersicurezza Nazionale (ACN) and Italian National CSIRT.

Continuous Threat Monitoring
24/7 monitoring of cyber threats is a fundamental pillar of Hera's strategy. By using advanced systems for incident detection, analysis, and response, the company can promptly identify abnormal behaviour, intrusion attempts, and potential attacks, intervening swiftly to minimise any impact. Hera's Security Operations Centre (SOC) ensures constant and coordinated oversight of all critical infrastructure (both IT and OT), integrating information from both internal and external sources.

Exercises and Training to Improve Cyber Risk Response
To strengthen its ability to respond to cyber incidents, Hera is increasing exercises and simulations activities involving internal staff, technical teams. These activities allow testing of response plans, evaluation of the effectiveness of operational procedures, and improvement of collaboration between different company units. Additionally, Hera invests in training and awareness programmes to promote a culture of security at all levels of the organisation.