Once built according to the above described assumptions, a security strategy should significantly reduce the number of potential cyber attackers to only a very small group of experts. Such expert are those whose knowledge, budget and time allow to break any security using methodologies that are transparent to monitoring systems. In fact, in practice, the high probability of being detected at the first error committed during attack should be an effective deterrent. This should discourage the vast majority of attackers to implement attacks. Nevertheless other methods to perform an attack, for instance using physical attack, may still be as effective as the (discouraged) cyber-attack.
Particularly, in the considered Italian Use Case, defence in depth implementation leads to *divide the considered system into security zones*, according to its functionality and criticality and to its physical location. This means to *identify security zones by grouping of logical or physical assets that share common security requirements*.
To establish a certain level of trust, a zone requires that all resources inside its borders have a certain minimum level of security as determined by the organization's security policies. In order to ensure a high security zone the trust level must be very high.
The main countermeasures to be adopted can be summarized as follow:

- Deploying anti-(D)DoS devices and services;
- Traffic filtering;
- Utilising timely patch management;
- Deploying anti-virus software;
- Performing system hardening;
- System & network segregation;
- Use of "demilitarized zones" (DMZs);
- data warehousing in order to facilitate the secure transfer of data from the SCADA network to business networks;
- Commissioning penetration testing and vulnerability assessments to third parties could provide an objective analysis of the level of security of a SCADA network.

After the selection of necessary countermeasures, it was necessary to verify how they were dealed with by the most relevant and mature standards. This analysis was conducted on one standard specific for the energy sector (NERC), two standards/guidelines on the information system (ISO/IEC 27001 – *Information Technology – Security Techniques* and NIST 800-53 – *Recommended security controls for information systems*) and finally two standards on ICS (ISA 99-03-02 – *Security for Industrial Automation and Control Systems* and NIST 800-82 – *Guide to Industrial Control Systems Security*). All those standard recommend similar countermeasures, although some technical or procedural details may differ.
Coming to the Polish case, a set of 211 countermeasures has been identified, including:

- a set of 54 countermeasures, which act to block feasibility of remote attack by unauthorized persons (remote attack means that was realized from different system than attacked),
- a set of 78 countermeasures, which act to block possible local attack (with physical access to console of a system or its products) either by staff or by unauthorized persons,