ESSENCE

***E**merging **S**ecurity **S**tandards to the **E**U power **N**etwork controls and other **C**ritical **E**quipment*

A project financed under the programme "Prevention, preparedness and consequence management of terrorism and other security-related risks" HOME/2011/CIPS/AG

The Essence project is a study to evaluate costs and benefits of the implementation of security standards to critical electric infrastructure, based on two case studies.
Networked computers reside at the heart of critical infrastructures, these are vulnerable to cyber attacks that can inhibit their operation, corrupt valuable data, and expose private information. Such attacks might affect large portions of the European power system, make repair difficult and cause huge societal impact, so that pressure to ensure cyber security of control and communication systems is now very strong worldwide. To that aim, several frameworks have been developed or are under development at present, both in the form of guidelines and proper standards, but it is difficult to evaluate costs and benefits of their adoption, although experimentation so far has shown that they may be huge.
In this scenario the key objectives of ESSENCE include:

1. Developing a common understanding of industrial needs and requirements regarding the security of control systems and the related standardisation efforts;
2. Identifying power system vulnerabilities induced by control systems, and estimating the likely socio-economic impact of failures due to faults and attacks exploiting those vulnerabilities;
3. Evaluating emerging frameworks for ensuring industrial control systems security, and establishing the costs of their adoption on an objective basis;
4. Recommending a pathway towards adoption of one or more of the above frameworks to the European power system infrastructure, having specific regard to EU transnational infrastructures as defined by the Directive 2008/114/EC.

The results of the project have been published in the “Special Essence series on security standards for critical infrastructures”, hosted in the “Ceris Technical reports series”. The published titles, available at http://essence.ceris.cnr.it/index.php/documents/2-uncategorised/14-reports, are:

1. Considerations on the implementation of SCADA standards on critical infrastructures of power grids.
2. Attack scenarios. Threats, vulnerabilities, and attack scenarios along with their selection criteria.
3. Terms of reference for the trials.
4. Benefit analysis. Assessing the cost of blackouts in case of attack. Evaluation based on Italian and Polish case study.
5. Cost analysis of standard implementation in the SCADA Systems of electric critical infrastructures.
6. Italian Case Study: socio-economic impact analysis of a cyber attack to a power plant in an Italian scenario. Cost and benefit estimation of CIPS standard adoptions. A reduced version.
7. Polish case study. Scenario based assessment of costs and benefits of adoption of comprehensive CIP standards.
8. Trial evaluation: conclusive lessons from Essence case studies.