1. INTRODUCTION

1.1 Scope of this report

The Essence project, funded by the CIPS EU programme, was designed to evaluate costs and benefits of applying emerging security standards to the European power grid controls systems, based on two case studies. Industrial control systems are vulnerable to cyber-attacks that might affect large portions of the European power system, due to the interconnection of this last, making repair difficult and causing huge societal and economic impact. To counter this threat, which is common to several networked infrastructures such as the oil and gas and the water networks, as well as power, oil and chemical process plants, several standard frameworks are being proposed.

When more than two years ago this project has been conceived, a lot of work on the definition and also on the technical assessment of standards against malicious attacks had been done. Nevertheless, in Europe no clear position had emerged and, even, some standards had failed to be completed for years. Substantially it was hard to come to a full stop, because of many reasons, but one of them was the lack of concrete experience on what generalized standard compliance would imply. The USA experience showed that applying a standard is cumbersome and costly, that benefits are unclear and their perception depends a lot on the political mood of the period. But how much this judgment could be transferred in Europe was unclear as well. In Europe the actual situation of the electricity infrastructure is generally more updated, but the public opinion has a lower appreciation of security and defence countermeasures.

The idea that moved the promoters of the project was that, to exit this impasse, two dimensions were necessary:

- *Concreteness*. Only a close look into some real electricity facilities could lead to detailed and grounded estimates of the impacts of standards for European utilities.
- *Multidisciplinary integration* of technical and socio-economic assessment[2]. To identify costs and benefits on an objective basis, it is necessary that the economic evaluation reflects precisely the detailed features of the compliance process on the one hand; and on the other that this assessment is based on the characteristics (time, duration, geographical area and type of customers involved) of the simulated blackouts caused by malicious cyber-attacks.

This report goes through the two Essence case studies, based on an Italian generation company and on the Polish Transmission System Operator (TSO) and browses the main findings of the two activities of analysis

[2] For this reason we accepted the challenge of integrating a very heterogeneous partnership, composed of:

- one multinational generation company (Enel) and one TSO (PSE), to consider the operation point of view.;
- furthermore two consultancy firms specialized in risk assessment and in security of the control systems in the electricity sector (ADC)
- from the socio-economic side, IEN, a research body specialized on energy and electricity, University of Western Piedmont, with competencies on utility regulation and management, and CNR, an Institute of CNR specialized in industrial economics, policy evaluation, and accountancy data management.