1. INTRODUCTION

Analysing costs of implementation of standards for the security of SCADA[2] systems of electric critical infrastructures is a complex exercise. Countermeasures included in standards are made of a complex mixture of hard and soft components, of new procedures and organisational assets. For this reason many cost items may be hidden and difficult to evaluate in their real extent. Only a simulation based on a real case study may lead to a realistic estimate. The variables are many, including the number of standards and of countermeasures to adopt, and there are several issues relating to each country and its characters. Thus it is important to start highlighting some relevant points, partly deriving from the case studies implemented in the context of the Essence project.

The first relevant fact to point out is the extreme complexity of protection, as possible attacks considered by standards encompass several layers of the network structure, distributed at several locations[3]. Besides the physical level has to be considered as well, and thus the need to protect the boundaries of the structures, and further threats deriving from personnel.

Moreover many countermeasures are encompassed in different standards[4]. This means that there is intersection between standards in terms of the presence of common countermeasures. Then, a relevant hurdle is the fact that costs of standards implementation might entail the cost of the same countermeasure in more than one standard. Thus the cost of single (possible very expensive) countermeasures might apply to more standards. These, in turn, describe uniform engineering or technical criteria, methods, processes, and practices and may actually be a regulatory requirement. The confusing proliferation of standards and guidance for electric power system cybersecurity has understandably made it more difficult for individual utilities to quickly determine what is required of them and has certainly posed a challenge for those who would like to review or provide input to the many parallel efforts. Since congruence between standards is great but not complete, a further line of analysis should assess the marginal effort to be borne by a firm who already decided to comply to one standard on a voluntary basis, in case another standard became mandatory. In the case studies we observed that standards like NIST, ISO, ISA/IEC are more or less compatible, but this comparison should in the future be made more precise. This detailed analysis could release the reluctance of electricity utilities to further invest on security against cyber-attacks, even on a voluntary basis.

A further conceptual hurdle is the fact that some countermeasures are more relevant than others. That is, some of the countermeasures that standards foresee are more important and effective than others, whatever the costs of implementation and maintenance. Thus, some controls and countermeasures are mandatory, while other ones can be considered as optional/additional. In consequence of this it is always important to properly identify the weaknesses existing in the single critical infrastructure (or to the local/national system)

---

[2] Supervisory Control And Data Acquisition

[3] For a carefully presentation of the impact of malicious incidents, or natural ones, on the main layers of an electric system, please see Antonio Diu (2014), "Terms of reference for the trials" Ceris technical report, special Essence series N. 51. http://www.ceris.cnr.it/ceris/rt/RT_51.pdf

[4] For a review of reviews the main existing or forthcoming standards that can directly or indirectly concern the power systems -analyzing their matureness, wideness and specificity of scope, points of strength and weakness – please see Ugo Finardi, Elena Ragazzi and Alberto Stefanini (2013), "Considerations on the implementation of SCADA standards on critical infrastructures of power grids". Ceris technical report, special Essence series N. 47. http://essence.ceris.cnr.it/images/documenti/RT_47.pdf