at the point of application of standards. This is useful to evaluate vulnerabilities and then possible risks, and then – once identified them – to implement the correct countermeasures.

It must also be noted that cyber systems used to operate power facilities differ substantially from those commonly implemented in ICT and, thus, also security differs in large scale.

The first, main difference is due to a fact that has a very high impact on the security of SCADA system of electric critical infrastructures. That is, technologies are often used for a time much longer than their usual lifetime in general IT companies. A meaningful example is that of Microsoft Windows XP operating system. This is still commonly exploited inside Intelligent electronic devices and in the office system of the automation sector. Nevertheless its support by the producer has ceased in April 8th, 2014. In power stations equipment this operating system will instead be at work for many years after its cessation.

This fact is mainly due to high costs of substitution. In turn, these high costs are first of all those of equipment and of workload of specialists. Then there are also costs depending on the need to stop the infrastructure in order to dismantle the equipment and then to replace it, program it and test it. Moreover there is a relevant need of continuity (plants can't be fully stopped), of precision of time parameters of devices and of reliability of communications. Finally, in the case of power facilities it is not possible to break operational services.

Costs for the implementation of security standards are of different types. First of all, fixed costs, independent on the number of critical infrastructures to protect, exist. Such costs are relative to the complex of the system (regional, national etc.) to be protected. A second type of costs are those that are scalable as they are relative to the single infrastructure, and thus depend on how many infrastructures must be protected.

Moreover, besides costs of initial implementation, also costs of maintenance and continuous upgrading must obviously be taken into consideration. Such running costs encompass costs for personnel as well as costs for the maintenance of physical infrastructures, of hardware and of the software.

A final important note is relative to the state-of-the-art of SCADA systems security in the critical infrastructures of different operators in different countries. It is rather obvious that, at the present stage, every operator has already implemented some security instruments in order to reduce the vulnerability of the systems. Thus, as Essence case studies show, attaining a common level of security following the common adoption of standards at European level will, in general, entail in practice lower (or even much lower) costs than starting from an hypothetical 0 level. This independently from which standard or guideline will become mandatory because, as reported above, several countermeasures are encompassed in more than one standard.

2. EVIDENCE FROM THE CASE STUDIES

The last years have witnessed an escalation of cyber-attacks. These have become more copious and much more sophisticated, and their consequences have been more catastrophic. Thus it is in the interest of enterprises to multiply efforts in order to overcome the consequences of possible attacks due to failures in the information security systems. These breaches can result in attacks affecting infrastructures and possibly compromising data of key value.

As above underlined, general information system security present differences with security for industrial automation and control systems. In the latter, requirements for integrity, availability, performance, and immediate access are higher. Moreover potential impacts of an attack on such systems might entail, besides