Polish case study. Scenario based assessment of costs and benefits of adoption of comprehensive CIP standards.

Hanna Bartoszewicz-Burczy [a], Clementina Bruno[*],
Fernando García [b], Tadeusz Włodarczyk [c]

*Corresponding author: Dipartimento di Studi per l'Economia e l'Impresa
Università del Piemonte Orientale
28100 NOVARA – ITALY
Mail: clementina.bruno@eco.unipmn.it

ABSTRACT: The Polish case study describes results of simulations of cyber-attacks on the Polish transmission system of electricity and compares the economic and social impact of these attacks, assumed to occur in situations where the system is working in normal operation, versus situations where standards are implemented as additional security countermeasures and the same incident arises. This work analyses security measures defined in selected documents, standardization, evaluates their effectiveness relative to attack scenarios, as well as implementation costs in comparison to weight of potential losses resulting from non-implementation. On this basis, a list of recommended safety measures, which guarantee high level of security and the highest level of return, has been prepared.

KEYWORDS: cyber security, malicious attack, power control centre, hardware breakdown, security standards, power threats, scenarios definition.

JEL CODE: D12, D61, L94.

[a] IEN - Institute of Power Engineering, 9 Mory str., 01-300 Warsaw, Poland
[b] Deloitte Advisory SL, Plaza Pablo Ruiz Picasso, 1, Torre Picasso, 28020 Madrid Espana
[c] PSE Operator SA, Warszawska 165, 05-520 Konstancin-Jeziorna, Poland