Practical Cybersecurity assessment of European Smart Grids

Sergei Gordeichik[1]
[1]*Scada Strangelove Research Team*

Modern Smart Grid implementations contain large numbers of system-wide and specific vulnerabilities both in individual components and in overall ICS systems and networks. Identifying and using these vulnerabilities requires an average level of expertise and a modest level of funds. The implications of such attacks may vary from local fraud to negative physical impact on power substation components to large-scale network accidents.
This research presents the findings of several projects aimed at assessing the security of different elements of electrical grid such as network communications, relay protection, SCADA, application software, small-scale power generation systems. Details of technical vulnerabilities and related cyber-physical attack scenarios will be discussed.