Cyber security threats \#x2014; Smart grid infrastructure

Submitted by grigby1 on Mon, 11/27/2017 - 12:25pm

Title	Cyber security threats \#x2014; Smart grid infrastructure
Publication Type	Conference Paper
Year of Publication	2016
Authors	Pandey, R. K., Misra, M.
Conference Name	2016 National Power Systems Conference (NPSC)
Date Published	dec
Keywords	composability, computer security, cyber infrastructure, cyber security, cyber security threats, cyber-attack, Demand response (DR), denial-of-service (DoS), electronic devices, ICT, ICT driven power equipment massively layered structure, Metrics, new generation sensors, NIST, Peak Load Management (PLM), power grid vulnerability analysis, power system framework, power system security, prosumer, Protocols, pubcrawl, R and D, Resiliency, risk evaluation process, SCADA, secure cyber infrastructure, security of data, smart devices, smart grid infrastructure, Smart grids, smart meters, smart power grids, smart power system, Software, WANs

Abstract

Smart grid is an evolving new power system framework with ICT driven power equipment massively layered structure. The new generation sensors, smart meters and electronic devices are integral components of smart grid. However, the upcoming deployment of smart devices at different layers followed by their integration with communication networks may introduce cyber threats. The interdependencies of various subsystems functioning in the smart grid, if affected by cyber-attack, may be vulnerable and greatly reduce efficiency and reliability due to any one of the device not responding in real time frame. The cyber security vulnerabilities become even more evident due to the existing superannuated cyber infrastructure. This paper presents a critical review on expected cyber security threats in complex environment and addresses the grave concern of a secure cyber infrastructure and related developments. An extensive review on the cyber security objectives and requirements along with the risk evaluation process has been undertaken. The paper analyses confidentiality and privacy issues of entire components of smart power system. A critical evaluation on upcoming challenges with innovative research concerns is highlighted to achieve a roadmap of an immune smart grid infrastructure. This will further facilitate R&d; associated developments.

URL https://ieeexplore.ieee.org/document/7858950/
DOI 10.1109/NPSC.2016.7858950
Citation Key pandey_cyber_2016

composability computer security cyber infrastructure cyber security cyber security threats cyber-attack Demand response (DR) denial-of-service (DoS) electronic devices ICT ICT driven power equipment massively layered structure Metrics new generation sensors NIST Peak Load Management (PLM) power grid vulnerability analysis power system framework power system security prosumer Protocols pubcrawl R and D Resiliency risk evaluation process SCADA secure cyber infrastructure security of data smart devices smart grid infrastructure Smart Grids smart meters smart power grids smart power system Software WANs