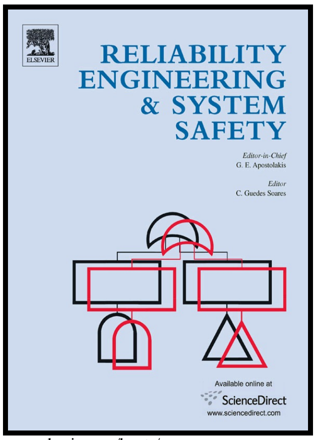

www.elsevier.com/locate/ress

Optimizing Power System Investments and Resilience against Attacks

Yiping Fang, Giovanni Sansavini

PII: S0951-8320(16)30724-4
DOI: http://dx.doi.org/10.1016/j.ress.2016.10.028
Reference: RESS5675

To appear in: *Reliability Engineering and System Safety*

Received date: 27 April 2016
Revised date: 14 September 2016
Accepted date: 30 October 2016

Cite this article as: Yiping Fang and Giovanni Sansavini, Optimizing Powe System Investments and Resilience against Attacks, *Reliability Engineering an System Safety,* http://dx.doi.org/10.1016/j.ress.2016.10.028

Optimizing Power System Investments and Resilience against Attacks

Yiping Fang[1], Giovanni Sansavini[1*]

[1]*Laboratory of Reliability and Risk Engineering, Institute of Energy Technology, ETH Zurich, Leonhardstrasse 21 8092 Zurich, Switzerland*

[*]*Corresponding author: Tel.: +41 44 632 50 38. sansavig@ethz.ch*

Abstract:

This paper studies the combination of capacity expansion and switch installation in electric systems that ensures optimum performance under nominal operations and attacks. The *planner-attacker-defender* model is adopted to develop decisions that minimize investment and operating costs, and functionality loss after attacks. The model bridges long-term system planning for transmission expansion and short-term switching operations in reaction to attacks. The mixed-integer optimization is solved by decomposition via two-layer cutting plane algorithm. Numerical results on an IEEE system shows that small investments in transmission line switching enhance resilience by responding to disruptions via system reconfiguration. Sensitivity analyses show that transmission planning under the assumption of small-scale attacks provides the most robust strategy, i.e. the minimum-regret planning, if many constraints and limited investment budget affect the planning. On the other hand, the assumption of large-scale attacks provides the most robust strategy if the planning process involves large flexibility and budget.

Keywords: Electric power network protection; System resilience; Transmission switching; Attacks; Trilevel optimization

1 INTRODUCTION

Electrical transmission networks (ETNs) are critical infrastructures (CIs) [1, 2]. Modern societies critically depend on their seamless operation for transmitting electric energy usually from remote generation plants to densely populated areas. Motivated by sustainability concerns, many governments enforce regulations that increase the fraction of energy generation from renewable energy sources (RES). For example, the Swiss Federal Council has developed a long-term energy policy ("Energy Strategy 2050") to gradually phase out nuclear energy, which amounts to around 39% of the country electric generation, and substitute it mainly by RES such as hydro, solar and wind power [3]. Germany has also increased the RES generation in the electricity sector from 6.3% in 2000 to about 30% in 2014 [4] and the RES share is expected to reach 80% by 2050 [5]. However, infrastructure investments needed to accommodate a massive share of RES into the