CYPRESS

# Arbitrating between preventive and corrective cyber-physical risk mitigation

Task 3.1 - Project Report

Efthymios Karangelos, Amirreza Jafari Anarjan, Louis Wehenkel

Date: November 2023

# Contents

# Executive Summary

The CYPRESS project aims at developing novel knowledge, methods and tools needed to help ensure the security of supply through the transmission grid, while accounting for the specific nature of cyber-threats and integrating them into a coherent probabilistic risk management approach. It is articulated along three research themes, aiming to develop: i) novel models and benchmarks for computer simulation and laboratory testing of the cyber-physical electric power system security of supply, ii) techniques for assessing the cyber-physical security of electric energy supply, and iii) techniques for enhancing the cyber-physical security of electric energy supply. The project scope falls entirely within the category of "fundamental research" within the meaning of Regulation (EU) No 651/2014 because it is experimental and theoretical work undertaken essentially with a view to acquire new knowledge on the foundations of phenomena or observable facts. The project is not intended to develop commercial tools.

The work presented in this document has been performed in the frame of CYPRESS WP3, titled "Mitigation of cyber-physical security risks". The objective of CYPRESS WP3 is to develop methods and algorithms to help reducing the risk with respect to the cyber-physical vulnerabilities of the electric power system. The document is the outcome of task 3.1, titled "Arbitrating between preventive and corrective cyber-physical risk mitigation". The objective of this task was to extend multi-stage stochastic programming approaches that have already been proposed to arbitrate between preventive and corrective measures in the context of physical power system security, so as to cover cyber-threats and in particular malicious attacks. This includes investigating the possible mitigation measures that could be applied in preventive and/or in corrective mode and in fine proposing optimization problem formulations that allow one to arbitrate among them in a well-informed way.

Following an introductory chapter, the 2nd chapter of this report provides a brief overview to the application of multi-stage stochastic programming in the context of electric power system (physical) security management. The purpose is to establish the necessary background for the extension of such approaches towards cyber-physical security management. This is done by stating model-agnostic stochastic formulations for the interrelated problems of power systems real-time operation and operation planning. Next, chapter 3 presents an investigation on both the cyber-physical threats facing the electric power system as well as the cyber countermeasures that may be deployed in preventive and/or corrective mode to counteract these. A review of the literature indicates that, up to nowadays, the focus of the research effort has been on single, precisely defined, threat instances rather than the (more general) problem of identifying the suite of countemeasures that should be put in place to sufficiently protect the system against the broad spectrum of unknown threats it faces.

Chapter 4 formalizes the extension of the multi-stage stochastic programming approach from the domain of physical security to the domain of cyber-physical security management. A main challenge

for this is the multitude of complex functionalities of the power grid cyber sub-system, in turn translating into a multitude of cyber-physical threats with diverse modeling requirements. We have inevitably opted for generality. More specifically, we first introduce a modeling abstraction of the power grid cyber sub-system as an interface between the physical procesess of electricity generation, transmission and distribution and the power system operator. We next use this modeling abstraction to state model-agnostic formulations for the decision making problem of malicious cyber-physical attackers[1]. We finally take a step back in time and discuss alternative generic formulations for the decision making problem of a so-called cyber-physical operation planner (a.k.a. security manager). This actor is seeking to identify optimal preventive/corrective cyber and physical security measures and while facing uncertainty on the properties of the malicious actor threatening the power grid.

The next steps in this research effort are discussed in chapter 5. The continuation of the CYPRESS WP3 research effort concerns both the precise mathematical models that should be used to formulate relevant instances of these stochastic problems as well as the development of proof-of-concept solution approaches.

## Author contributions

Efthymios Karangelos is the author of chapters 1, 2,4,5 and co-author of chapter 3 and appendix A. Amirreza Jafari Anarjan is a co-author of chapter 3 and editor of the report. Louis Wehenkel is a co-author of appendix A and editor of the report.

| Author | Affiliation |
|---|---|
| Efthymios Karangelos (Task leader) | Université de Liège |
| Amirreza Jafari Anarjan | Katholieke Universiteit Leuven |
| Louis Wehenkel | Université de Liège |

Table 1: List of Authors

[1] An instance of such model-agnostic formulation, specifying precise models and data as well as the strategy and motivation of a cyber-physical attacker is given in Appendix A.

This project is supported by the Belgian Energy Transition Fund