CYPRESS

Deliverable 3.4

Electric power system cyber-physical risk mitigation: lessons learnt through fundamental research and stakeholder interaction

Raphael Fonteneau, University of Liège
Louis Wehenkel, University of Liège
Efthymios Karangelos, University College Dublin

Date: September 30, 2025

Contents

Executive Summary

This deliverable proposes recommendations regarding the mitigation of cyber-physical risks of the bulk electric energy supply system. Nourished both by research developed within the scope of the CYPRESS project and by expertise shared by stakeholders from the regulated and non-regulated sectors, this deliverable is structured into two main parts: the first part presents the main research outcomes of the CYPRESS project, while the second part synthesizes the expert sharing exposed during the workshop series. This deliverable finally discusses points of convergence between the different sources, and to this respect, identifies - among others - the question of the interplay between the use of new technologies and the human factor. This includes, for instance, the development of decision support tools for human operators to help mitigating cyber-physical risks, or the design of real-time simulation tools to train operators, who remain the last line of defence against cyber-physical attacks.

1

Introduction

The CYPRESS project[1], which started in November 2020, aims to develop novel knowledge, methods, and tools needed to help ensure supply security 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 (also known as mitigation strategies).

The objective of this deliverable is to identify recommendations that come out of the CYPRESS project for mitigating cyber-physical threats and which may target electric power system stakeholders who collaborate with TSOs. More concretely, the recommendations provided in this deliverable have been nourished through two main channels: the first channel is the fundamental research itself, which was elaborated within the CYPRESS consortium. The second channel is the expertise of stakeholders who have shared their views during two workshops[2]. After exposing the key points of each source of information, we synthesize some essential recommendations, trying to keep them as non-technical as possible, to finally try to discover common denominators among all recommendations. Among those, the interplay between the human factor and new technologies stands out as a keystone. We identify at least two types of such interplays: first, the design and integration of technologies dedicated to support human decision making, and second, the use of real-time simulators to train operators and increase their intrinsic skills to react to cyber-physical attacks. Finally, while being more related to the evaluation of mitigation strategies rather than on their design, the use of simulation and co-simulation platforms plays an important role in the overall process of enhancing cyber-physical security.

[1] Webpage of the project: `https://cypress-project.be/`

[2] See the webpage of the CYPRESS Workshop Series: `https://sites.google.com/view/cypressworkshopseries`

The rest of this deliverable is organized as follows: relying on the deliverables and publications produced during the project, Chapter 2 presents a recommendation-oriented synthesis of the CY-PRESS project regarding the mitigation of cyber-physical risks of electric power systems. Chapter 3 synthesizes the stakeholders' views shared during the workshops. Chapter 4 discusses some common denominators between elements detailed in Chapters 2 and 3, while Chapter 5 concludes the paper.

2

A research journey

As a fundamental research project, the CYPRESS project has been structured around four three main research directions: (i) a first direction dedicated to elaborating criteria and benchmarks for cyber-physical risk management, (ii) a second direction focusing on cyber-physical risk assessment, with the objective to develop a coherent methodology for the assessment of cyber-physical risks and (iii) a third direction about mitigating cyber-physical security risks, with the goal of developing methods and algorithms to help reducing the risk with respect to cyber-physical vulnerabilities.

More specifically, the third research direction, which has focused on mitigating cyber-physical risks, has delivered several outputs that we aim at synthesizing into recommendations in the following subsections. It has been structured along 3 main research questions: the question of arbitrating between preventive and corrective strategies, the question of enhancing the real-time operation cyber-physical security, and the question of enhancing cyber-physical security in look-ahead mode. In the following sections, we summarize and extract recommendations for each of these questions.

2.1 Deliverable 3.1 - Arbitrating between preventive and corrective cyber-physical risk mitigation

The first research question to be explored was the extension to the domain of cyber-physical security of some classical methods - mainly relying on multi-stage stochastic programming techniques - originating from the domain of physical security to the context of the arbitrage between preventive strategies and corrective strategies [1], [2]. Preventive measures include, for instance, choosing the transmission grid topology, the dispatching of power generating units, or the settings of automatic protection devices. In the context of physical electric power grid security, preventive security management means taking decisions before any credible contingency event happens so as to ensure that the system can resist to this event without any further intervention from its operator. This extension

to cyber-physical security, detailed in Deliverable 3.1 of the project [3], entails:

1. ensuring that the design of the cyber sub-system may not induce any contingency events that cannot be quickly addressed by the operator of the electric power grid,

2. adapting the physical controls of the electric power grid to be able to resist to a broader set of credible events, including contingencies induced by malfunctions of the cyber sub-system.

From this research, some key recommendations can be identified:

- *Choosing the right scale:* there is a need to model the cyber sub-system of the power grid at a suitable level of detail taking into account the diversity in threats and countermeasures. A cyber sub-system modelling abstraction, focusing on the effect of cyber threats on the interface variables between the physical components, the cyber sub-system as well as the human operators (and control automata) of the power grid, has been introduced.

- *Getting to know the enemies:* most relevant cyber-physical threats are not exogenous fatal contingencies but rather intentional malicious attacks designed by intelligent agents. An effort has been done to describe the characteristics of these agents by defining a sort of taxonomy of cyber-attackers, who differ by their motivations, resources, understanding and modelling skills regarding the cyber-physical electric power system.

- *Managing mathematical and algorithmic complexity:* considering the two previous items when designing a decision making framework, as it has been proposed in [4] in the form of a tri-level optimization framework including a cyber-physical planner, and cyber-physical attacker and a power grid operator, opens many questions related with computational costs. Working on algorithmic efficiency, and also exploring alternative decision making approaches such as for instance Multi-Agent Reinforcement Learning [5], in particular in an adversarial context, is recommended for future research.

2.2 Deliverable 3.2 - Enhancing Cyber-Physical Security in Real-Time Operation

The second research question has focused on the production of a coherent set of results and tools contributing to the enhancement of real-time cyber-physical risk mitigation techniques. In a global picture, a choice has been made to explore how diagnostic tools, anomaly detection mechanisms, and cyber-resilience frameworks could be integrated into the real-time operation of power systems. Several topics have been investigated: development of diagnostic agents extracting key features from cyber-infrastructures, development of IT anomalies, characterization of cyber-operators and identification of preventive and corrective actions they may take, and finally, design of cyber-attack resilient cyber-physical systems that could maintain their functionality even when the underlying ICT infrastructure is partially compromised.

From this research, which is comprehensively detailed in Deliverable 3.2 [6], some key recommendations that could be emphasized are the following:

- *Thinking as a whole and minding the interface:* since threats often exploit interdependencies and interfaces between components, holistic approaches for securing cyber-physical systems should be favoured.

- *Keeping the human in the loop:* human operators are the key to maintaining the overall system in operation: they must receive dedicated training and be provided with reliable decision-making tools.

- *Thinking corrective strategies as adaptive and capable of generalisation:* while proactive strategies play a vital role in reducing vulnerabilities, real-time adaptive decision-making during incidents may ensure better responses against unforeseen threats. This balance should be sought in a collaborative and multidisciplinary manner between teams spanning IT, electrical engineering, and operations.

2.3 Deliverable 3.3 - Enhancing cyber-physical security within look-ahead mode

The last fundamental research question that was investigated is the so-called look-ahead mode, which is, in essence, the question of the day-ahead operation planning. An approach close to the reality of the European electricity system has been followed, where multiple TSOs operate an interconnected grid by looking after its several control-areas, and need to exchange information, while potentially exposing themselves to cyber threats. In this context, a day-ahead Cybersecurity Constrained Optimal power flow (CSC-OPF) framework has been proposed.

The proposed approach integrates a bi-level attacker-defender formulation into the day-ahead cybersecurity-constrained dispatch model. The upper level models the attacker, while the lower level models the system operator's response: the goal of the attacker is to identify a subset of power system components to compromise, while the goal of the system operator is to minimise financial costs and lost load induced by the attack.

The novelty of the exploration of this research question is twofold. First, taking into account the fact that TSOs are interconnected, it explores three different communication strategies between them: (i) a centralized coordination, where all TSOs jointly optimize the entire system with full knowledge of each other's topology and parameters, (ii) a non-coordinated planning, where each TSO independently optimizes its region without considering inter-area consequences and (iii) a decentralized coordination, which allows TSOs to optimize locally while sharing only essential information. The second originality of the work is the inclusion of a probabilistic framework by considering attack likelihoods derived from risk assessments, thus enhancing the efficiency of corrective plans against critical attack scenarios.

Some key recommendations that could be extracted from this research (comprehensively described in Deliverable 3.3 [7]) are the following:

- *Favouring decentralized coordination:* by avoiding the complete data sharing across TSOs, the decentralized coordination framework allows a better cyber-resilience of the grid by reducing the sharing of sensitive operational information without harming the economic and operational feasibility (operational costs being within 0.4%–0.6% of those obtained via centralized coordination).

- *Considering likelihood rather than worst case analysis:* This allows for the prioritization of attack scenarios that are not only highly disruptive but also realistic in terms of occurrence probability. The resulting optimization process improves the defender's level of preparation by allocating corrective resources where they are most likely needed.

2.4 Focus on research articles

For interested readers, we would like to highlight the two following articles elaborated from the research carried out within the framework of the Cypress project.

The first article [8] proposes an innovative anomaly detection (AD) method capable of identifying cyberattacks at their earliest stages, before they impact power grid operations. Rather than inspecting data content, the proposed system analyses network communication patterns, specifically the timing and intensity of data flows between devices. By applying advanced signal processing techniques, subtle variations in network traffic behaviour are detected and extracted as distinctive features. These

Figure 2.1: Illustration of the independent decision-making actors involved in the tri-level optimization framework proposed in [4] - credits: E. Karangelos and L. Wehenkel

features are further analysed by a specialized hybrid deep learning architecture, which captures critical relationships and temporal dependencies across network nodes. This approach effectively identifies stealthy attack scenarios, such as low-rate Distributed Denial-of-Service (DDoS) attacks and covert network scanning activities, which are traditionally challenging to detect. Evaluated through simulations of IT-OT networks under a wide range of attack scenarios, the proposed method demonstrates superior accuracy and reliability compared to traditional AD algorithms which focus on identifying anomalies through analysing spatial and temporal patterns derived from the physical system measurements.

The second article [4] discusses the security of electric power transmission grids against malicious cyber-physical attackers, who exploit digital systems to disrupt electricity supply. A crucial premise of the research is that cyber-security measures are not perfectly effective; highly skilled attackers may eventually find ways to bypass them. To address this, the paper proposes an integrated cyber-physical risk management framework. This framework involves selecting preventive security measures in a combined manner, and specifically:

- Physical security measures, such as procuring reserve power capacity from generators.
- Cyber-security measures, like updating firewall rules to impede intruders from taking over cyber infrastructure.

The primary finding is that physical and cyber-security measures are non-exchangeable complements. They must be chosen in an integrated manner for effective grid security. For instance, if an attacker can bypass cyber-security, stronger physical measures become crucial to ensure the grid's security. This combined approach is essential to help the grid better withstand diverse threats.

3

Stakeholders feedback

As part of the work plan of the CYPRESS project, two workshops have been organised during the last year of the project on the topic *Cyber-Physical Risk of the bulk Electric Energy Supply System: Enhancing Multilateral Co-responsibility* with the following objectives: (i) to invite actors of the bulk electric energy supply system to hear about their fears / rules of good practice regarding cyber-physical risks, (ii) to disseminate results from the CYPRESS project and make some connections with (i) and (ii) to engage general discussions. These workshops have been set up to hear the voice of main actors of the bulk electric energy supply system, including experts from the regulated and non-regulated sectors. The speakers have shared their vision and/or the vision of their organisation on the previous points (i) and (ii), and we hereafter synthesize such perspectives.

3.1 Perspective from the public, regulated and non-profit sectors

The utilities, including TSO and DSOs, play an important interfacing role with many entities: between technology and services providers, electricity producers and consumers. As operators of the electricity networks, they hold a specific responsibility to make the whole system efficient and reliable, under the guidance and control of different public entities, including regulators or international organizations such as ENTSO-E. As a common perspective shared among all sectors (regulated, non-regulated, non-profit), there is a shared sense of responsibility to make the overall electric energy supply system secure with respect to cyber-physical risks.

3.1.1 Perspective from the Belgian Federal Public Administration

From the Belgian Public Federal Administration, the cyber-physical resilience of the bulk electric energy supply system should be viewed under the light of three paradigms. The first paradigm is the energy transition, which started more that twenty years ago. The second paradigm is the evolution

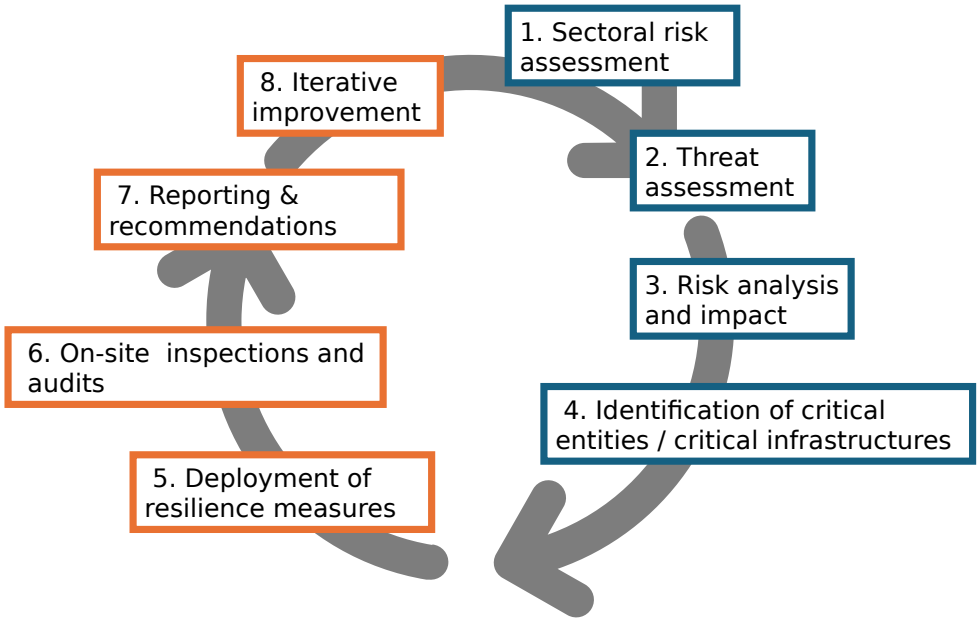

Figure 3.1: An iterative procedure for assessing and mitigating threats on critical infrastructure

of threat landscape, which has dramatically changed in the last three years. Some states have to be considered as potential threat actors, motivated by ideologies that are hostile to European democracies, and using hybrid war - involving spying, sabotage [1], interference. The third paradigm is the legal adaptation in the EU, which started with the European Programme for Critical Infrastructure Protection, and which is constantly adapting.

The Belgian Federal Administration is particularly concerned with the protection of critical infrastructures in the EU and the North Atlantic Alliance: from (semi) private market operators and complex networks to defence of the interests of the state, from national and international land, maritime and cyber domain to essential functions, societal expectations and delivery of public service. It follows some investigation guidelines, as well as some iterative assessment procedures (see Figure 3.1).

Belgium is collaborating both at the regional level (bilateral agreements, cross-border initiatives, North Sea Security Pact, North Seas Energy Cooperation[2]), at the European level (e.g., EU directives and recommendations, action plan on submarine cables), and within the North Atlantic Alliance.

The authorities expect from the operators a capacity of resilience in the delivery of essential services, through having critical entities resilience plan, scenario-based protection measures, practice of exercises, use of Information Security Management Systems (NIS2) or equivalent. On the other side, the operators expect from the authorities a clear definition of roles and responsibilities, a level-playing field, clear perspectives on the threat landscape, seamless communications with the authorities, external protection measures, support, funding and collaboration to implement new technological security measures.

The Belgian Federal Administration has identified several challenges and opportunities. Among the several challenges to be addressed, let us mention the supply chain complexity (e.g., availability of the spare parts, trusted third actors, repairing capacities), the urgent need to integrate security by design for the civil sector, the technical and legal response to emerging and new technologies. In particular, this asks the question of how the legal framework should evolve in order to support the arrival

[1] See, for instance, the recent attack on a Norwegian dam:
https://www.theguardian.com/world/2025/aug/14/russian-hackers-control-norwegian-dam-norway

[2] Link to The North Seas Energy Cooperation webpage:
https://energy.ec.europa.eu/topics/infrastructure/high-level-groups/north-seas-energy-cooperation_en

of technologies within society while ensuring the preservation of cyber-physical security (e.g., drones, cloud data sovereignty, submarine cables, security guarantees on the use of AI, quantum computing). Regarding opportunities, they are also related with new energy technologies for enhancing the resilience of the EU and the North Atlantic Alliance, in particular in the domains of logistics, climate change, sovereignty and independence. These opportunities go both ways, to and from the electric energy supply system. As an example, windfarms and critical undersea infrastructures could be used to monitoring the maritime domain (e.g., distributed acoustic systems, radars, cameras, sensors). However, these opportunities are more related to the question of monitoring and assessment rather than on mitigation.

From the sharing of the Belgian Federal Administration, the following recommendation is emerging:

- *Strengthening collaboration between regulated and non-regulated sectors:* As the energy networks (electricity, gas, etc) are built, operated and maintained by non-regulated operators, and mostly market-designed, the action of public authorities to increase cyber-physical security is costly and not direct. A closer collaboration between the regulated (i.e., subject to specific rules and legal or administrative frameworks for the general interest) and non-regulated sectors, both on civil and military aspects, is required to go on with the settlement of an operational framework for the protection of critical infrastructures.

3.1.2 Perspective from the side of TSOs

In this subsection, we chose to group two feedbacks, one obtained from the Belgian TSO, the other by ENTSO-E, which is the association of TSOs among Europe. By their central position in the electric power grid, TSOs implicitly play the role of multi-technology integrators. From this reality, the perspective shared by the TSO has been structured along a list of seven points of attention, represented in Figure 3.2. These 7 points of attention are summarised hereafter:

1. In a trivial way, digitalization transforms isolated substations into networked systems and offers new entry points for potential threats. Technically, attackers can now manipulate physical equipment using the Operational Technology (OT) of the energy infrastructure.

2. Similarly to the previous point, IoT communication (e.g., connected sensors) also bring new vulnerabilities: attackers could perturb the observations, hide critical issues, potentially leading to the failure of the equipment, or even to larger consequences.

3. IT applications development cycles acceleration is a potential nest for security gaps, including for market applications. It is not science fiction to imagine a manipulation of prices on the electricity markets, leading to physical consequences, such as for instance, the hindering of renewable energy sources integration [9].

4. At the centre of all these points, the human factor is both a source of strength and vulnerability. Well trained operators may be the last line of defense in case of crisis, but on the other hand, social engineering can exploit authority and emergency to bypass crucial controls.

5. New decentralized assets, mainly pushed by the energy transition (solar PV, wind turbines, inverters, etc), introduce new risks: for instance, compromised offshore platforms could simultaneously disconnect GWs of power generation.

6. As new technologies emerge, it becomes almost impossible to enumerate the new threat opportunities (e.g., quantum computing, AI, autonomous systems, biometrics, edge computing) that reshape both threat landscapes and defensive capabilities across our critical infrastructure. Among the multiplicity of devices and software associated with these new technologies, some may be of a black-box nature, i.e. we may not know all the details behind how they work. In addition to this, some services may pose problems in terms of data sovereignty, for instance cloud

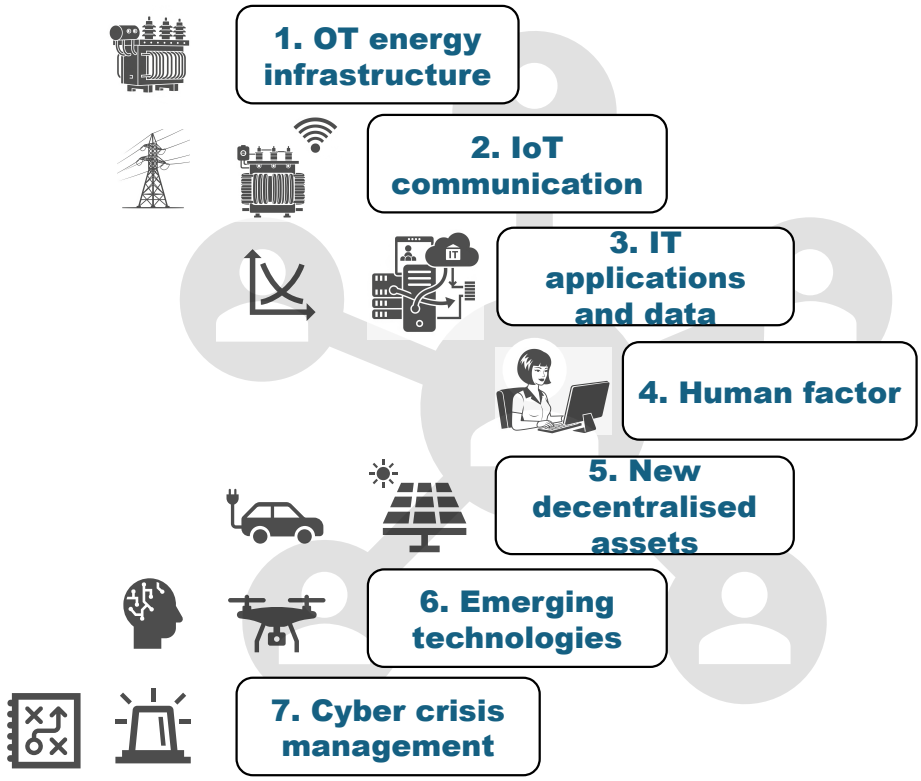

Figure 3.2: The TSO is at the crossroad of many sources of strength and vulnerabilities.

storage. The use of Non-EU solutions for storing or manipulating critical EU infrastructure data should be questioned.

7. Finally, the TSO needs to maintain, in parallel with robust preventive measures, comprehensive cyber crisis management capabilities, including tested protocols to ensure grid stability and rapid recovery in case of cyber incident.

TSOs are interconnected, primary to exchange electricity, but also, by force of circumstances, potential vulnerabilities. Asynchronous maturity between TSOs should be assessed, since the weakest grid determines the weakness of the common grid. Beyond simply equalizing the security level of maturity among TSOs, many actions could be taken to strengthen the cyber-physical security: shared incident databases, training, knowledge sharing and exercises, security-oriented investment decisions.

From the perspective of TSOs synthesized above, we formulate the following recommendations:

- *Minding the 3D : data, digitalization and decentralization:* the process of digitalization in conjunction with the deployment of decentralized assets increase the attack surface. AI and ML techniques are being used by the attackers, and should also be used by the defender side. Data sovereignty is becoming a growing issue.
- *Avoiding disparate levels of cyber-physical security maturity:* the strength of the weakest link becomes the strength of the whole. Official instances like ENTSO-E propose, among other things, concrete actions to help European TSOs move forward harmoniously.[3]
- *Working on strength and vulnerability of the human factor:* reinforcing the strength of the human factor, while diminishing its potential vulnerabilities should be a by-design characteristic of future decision making helper tools.

[3]See for instance, the TYNDP initiative which identifies gaps in infrastructure from a European perspective: `https://tyndp.entsoe.eu/`

3.1.3 Perspective from a DSO

DSOs share some common cyber-physical security challenges with TSOs. In particular, distribution networks substations should be seen as cyber-physical systems, featuring different network activities: protection relays, intelligent electronic devices, remote terminal units and switches. Protection parameters can be changed, disturbances are collected and recorded, etc. On the other hand, many physical security measures are already implemented: the distribution system is a multi-layered system, provided with airlock systems, video surveillance, intrusion detection systems, and environmental risks management.

DSOs have been concerned about building a resilient network for a while. Taking the example of Brussels' DSO (Sibelga), we can mention that the system is provided with its own optical fiber network since 2014, with nearly 280km installed ; there is a dedicated connectivity to substations (over 120 nodes) with real-time remote control capabilities, immune to traditional telecom disruption. There is an automatic re-routing system in case of cable failure, and back-up batteries allow to maintain node power during blackouts.

On the side of human factor, there is a growing need for hybrid skills encompassing both physical and cyber-physical awareness. Cyber-physical security should be considered as a collective effort, and part of this effort amounts in a cultural switch from thinking that it is an IT problem to realising that cyber-physical security is everyone's responsibility. DSOs have developed a strong culture of safety, and many good practice rules developed in the safety domain could be derived analogously in the cyber-physical security domain.

As recommendations, we retain the following elements:

- *Working on change management and cultural switch:* enhancing mitigation strategies for cyber-physical risks implies to increase staff competences and knowledge in order to extend safety culture to safety and cyber-physical security culture.

- *Holding continuity and evolution together:* the DSO strives to maintain the operability of the grid and manage conflicting timelines between network renewal rate and technology evolutions. The recommendation here is to continue to take care to keep together innovation and the maintenance of what already exists.

3.2 Perspective from services and technology providers

During the CYPRESS workshops, speakers from the non-regulated sector had the opportunity to share their views on the issue of co-responsibility in relation to cyber-physical risks. As main provider of hardware and software solutions, as well as services, some industries are specifically concerned by cyber-physical risks. Through the different solutions they bring to the market, companies explicitly and implicitly foster or disadvantage cyber-physical security. Actors from the non-regulated / market driven sector may be balanced between protecting their intellectual property and offering fully transparent solutions to facilitate their interpretability, which may encourage the use of open-source solutions. However, by over-exposing technical details, they may facilitate retro-engineering risks, and facilitate the work of malicious actors. This typically concerns AI and ML techniques, for which many potential solutions are accessible in the form of open-source python libraries offering the possibility to check the code.

Enhancing cyber-physical security may also open new business cases, for instance, for assisting other actors - including the utility - in assessing and enhancing their cyber-physical security. Such an illustration was provided by one of the stakeholders: the design of a real-time cyber-physical simulator of the French network, with two main objectives: testing new automata, and training the operators. To do so, they rely on an information flow-based co-simulation approach [10], which has the advantage of (i) requiring less data on the cyber-system, (ii) being computationally efficient (currently handling 500k messages per second on the French system on a laptop), and (iii) offering scalability

and adaptability. This real-time cyber-physical simulator already makes it possible to offer training to operators.

As a synthesized recommendation coming out of the perspectives shared by stakeholders from the non-regulated sector, we retain the following idea:

- *Being an actor of the improvement of cyber-physical security:* the idea is to contribute to the production of technologies and services to improve the cyber-physical security of the electricity supply system, in particular relying on new technologies such as AI and ML for which transparent, open-source solutions are available to the general public.

4

Discussion

This section aims to highlight points of convergence between the academic research that has been conducted within the CYPRESS consortium and the information shared during the CYPRESS workshops. For illustration purposes, we provide in Figure 4.1 a schematic representation of the different recommendations mentioned in Section 2 and 3. As a general and perhaps self-evident idea, innovation, which seems to be the main vector for the introduction of new entry points for cyber-physical threats, is nevertheless the main source of solutions to the problems created by these new threats. The power of these new tools, if used, must be accompanied by rigour in knowing their characteristics [1], potentialities and limits, which is probably more feasible in the case of open-source tools, even if it poses other challenges, such as, for instance, adversarial retro-engineering.

A second idea to emerge, is the role that the human factor is called upon to play in mitigating cyber-physical risks. This idea is closely related with the previous one: the proliferation of connected and potentially black-box hardware and software solutions could represent a threat in terms of cyber-physical risks in the event that these solutions are not either accompanied with some dedicated human training, or oriented towards human decision support. Among the recommendations related to the human factor, that of having closer collaborations between the different entities (regulated and non-regulated, related to physics or more with IT, between TSOs, etc) of the entire electric energy supply system was mentioned several times, in particular for keeping vigilance at the interface level (between technologies and between networks).

The search for points of convergence would be incomplete if we did not mention the aspects linked to the simulation and co-simulation work carried out within the framework of the project, also mentioned during the workshops, some of them being pushed even further outside the CYPRESS project.

[1] See, for instance, the case of rogue communication devices found in Chinese solar power inverters: `https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/`

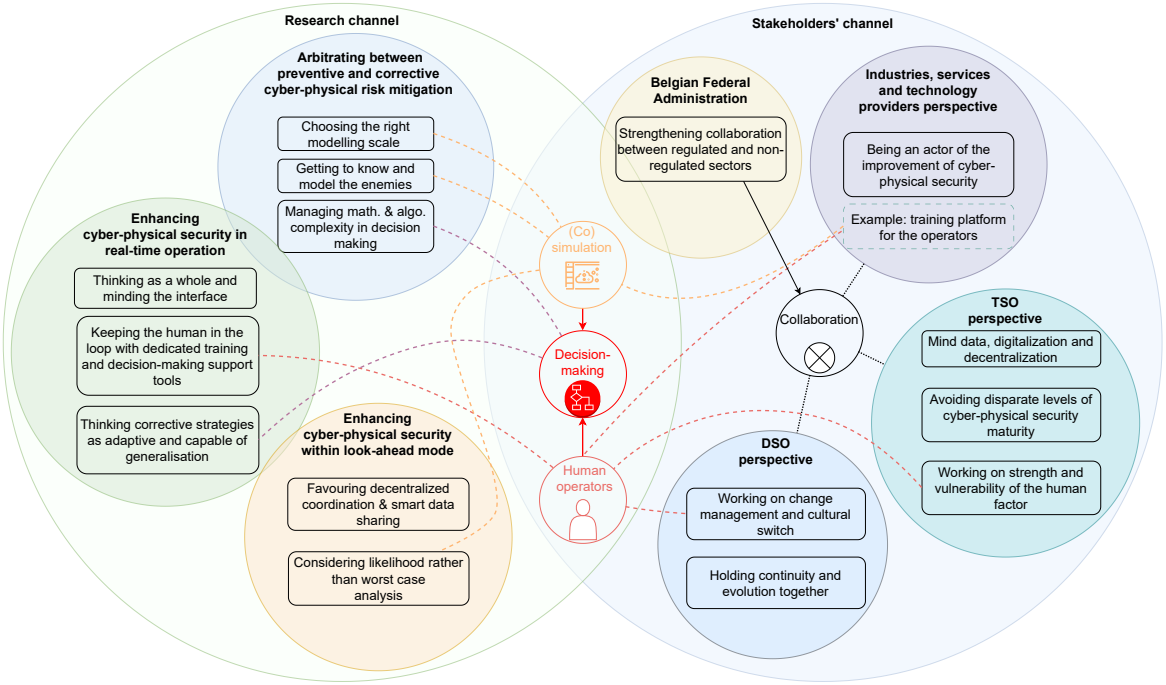

Figure 4.1: A schematic illustration of the recommendations coming out of the research and the stakeholders' perspectives. Dashed line indicate connections between recommendations, while arrows indicate a causality link (either already established, either suggested).

We believe that there is still room to explore regarding this family of tools [2]. Regarding the dedicated training of operators, the challenge lies in the real-time aspects. Regarding (co-)simulation tools, the challenge lies rather in the simulation of interactions between the cyber and physical layers.

During a panel discussion at one of the workshops, the idea of being able to carry out stress tests to combat cyber-physical risks was discussed. Stress-tests have been proposed after the 2008 bank crisis as *a tool to assess the resilience of the financial institutions to adverse market developments, as well as to contribute to the overall assessment of systemic risk in the financial system of the European Union* [3]. Developments of the CYPRESS project, in particular related with (co)-simulation, can be seen as the building blocks of such a stress test platform, even if there is still much to be done, both in terms of academic research, industrial developments, and cooperation between the different stakeholders involved.

During the the last CYPRESS workshop, the following question was asked to the panel of experts, which included people who participated in writing the CYPRESS proposal: *The CYPRESS project was elaborated before the beginning of the war in Ukraine. If the project was to be written right now, would it be written in the same way?* As a side-answer to this question, the following recommendation was formulated: *to work more on the 'cyber-physical restoration process'*. This could imply for example the definition of dedicated guidelines and procedures to help restore, in a coordinated manner, both the classical physical power system as well as the most critical (from the physical part perspective) cyber-subsystems.

[2] We can also mention the Horizon project TwinEU which aims at creating a concept of Pan-European digital twin of the electricity system based on the federation of local twins - see `https://twineu.net/`

[3] See, for instance, the dedicated page on the Belgian National Bank: `https://www.nbb.be/en/financial-oversight/prudential-supervision/european-system-financial-supervision/eu-wide-stress`

5

Conclusions

As the CYPRESS project is reaching to its end, this white paper aims to aggregate recommendations from academia and stakeholders on the possibilities of mitigating cyber-physical risks, and ultimately to open up prospects for future developments. The project has demonstrated that it was possible to formalise and provide quantitative answers to research questions related with the assessment and the mitigation of cyber-physical risks. Indeed, access to data and real models was limited, and many future works can be envisioned. The perspectives shared by stakeholders should be seen as aids in defining the outlines of such future work.

6

Acknowledgements

Thanks to (in alphabetical order) Alireza Bahmanyar, Daiga Dege, Benjamin Krikler, Frédéric Olivier, Ludovic Rigaux, Frédéric Sabot, Loïc Tilman, Guillaume Van der Schueren, Annemie Vermeylen for sharing their expertise during the CYPRESS workshops. Thanks to Tohid Behdadnia, Klaas Thoelen and Geert Deconinck for providing a summary of their research article. The responsibility of the content of this deliverable rests with its authors.

Bibliography

[1] F. Capitanescu et al., "State-of-the-art, challenges, and future trends in security constrained optimal power flow," *Electric power systems research*, vol. 81, no. 8, pp. 1731–1741, 2011.

[2] F. Capitanescu, "Critical review of recent advances and further developments needed in ac optimal power flow," *Electric Power Systems Research*, vol. 136, pp. 57–68, 2016.

[3] E. Karangelos, A. Jafari Anarjan, and L. Wehenkel, "Arbitrating between preventive and corrective cyber-physical risk mitigation," CYPRESS project, Tech. Rep., November 2023. [Online]. Available: `https://hdl.handle.net/2268/335561`.

[4] E. Karangelos and L. Wehenkel, "Electric power system security: The case for an integrated cyber-physical risk management framework," *Sustainable Energy, Grids and Networks*, vol. 43, p. 101 872, 2025.

[5] C. Li and M. Qiu, *Reinforcement learning for cyber-physical systems: with cybersecurity case studies*. Chapman and Hall/CRC, 2019.

[6] L. Mathy et al., "Enhancing cyber-physical security in real-time operation," CYPRESS project, Tech. Rep., January 2025. [Online]. Available: `https://hdl.handle.net/2268/335745`.

[7] A. Jafari, H. Ergun, and D. Van Hertem, "Enhancing cyber-physical security within look-ahead mode," CYPRESS project, Tech. Rep., June 2025. [Online]. Available: `https://lirias.kuleuven.be/4259330&lang=en`.

[8] T. Behdadnia, K. Thoelen, and G. Deconinck, "Early-stage anomaly detection in IT-OT power grid communication networks using wavelet transform and hybrid deep learning," *IEEE Transactions on Smart Grid*, 2025.

[9] G. O. Alsharif, C. Anagnostopoulos, and A. K. Marnerides, "Energy market manipulation via false-data injection attacks: A review," *IEEE Access*, vol. 13, pp. 42 559–42 573, 2025. DOI: `10.1109/ACCESS.2025.3548914`.

[10] Y. Cao, X. Shi, Y. Li, Y. Tan, M. Shahidehpour, and S. Shi, "A simplified co-simulation model for investigating impacts of cyber-contingency on power system operations," *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 4893–4905, 2017.

This project is supported by the Belgian Energy Transition Funds