

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

Cyber-Physical Risk Mitigation in Power Systems

By Raphael Fonteneau, Tohid Behdadnia, Geert Deconinck, Louis Wehenkel
and Efthymios Karangelos

This article proposes recommendations regarding the mitigation of cyber-physical risks of the bulk electric energy supply system. The paper is structured into two main parts: the first part presents outcomes from recent fundamental academic research spanning different timescales (preventive vs corrective risk mitigation, look-ahead planning, real-time operation), while the second part synthesizes some expert knowledge from stakeholders (Administration, TSOs, DSO, technology and service providers). For both sources of information, we extract high level, non-technical recommendations, and the paper finally discusses points of convergence between the different sources, and in 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 mitigate cyber-physical risks, or the design of real-time simulation tools to train operators, who remain the last line of defense against cyber-physical attacks.

Introduction

The bulk electric energy supply system is undergoing numerous changes, brought about in particular by the energy transition and liberalization, together associated with a digitalization process that runs through the whole society. This produces smarter and more efficient electric power systems in the form of Cyber-Physical Systems, where power grids are closely linked with a growing number of information and communication systems. This evolution has pushed the scientific community to develop new knowledge, methods, and tools to help protect the security of energy supply through the transmission grid, while also accounting for cyber threats and integrating them into a coherent probabilistic risk management approach.

Recent cyber incidents show why this is not only a theoretical concern. In 2015 and 2016, intrusions into the Ukrainian power sector led to real outages and highlighted how digital access can translate into

Version 03 - 15th February 2024

IEEE Power & Energy Magazine

Example Template for Draft Articles

physical impact^{1,2}. In 2017, the TRITON case showed that attackers can target industrial safety systems, with consequences that go beyond data loss or short service disruption³. In 2022, defenders reported stopping another attempt in Ukraine that involved grid-focused tooling^{4,5}, and in the same year the KA-SAT incident showed how a cyberattack on a communications dependency can disrupt remote monitoring and control at scale, including in the energy context⁶.

As these incidents become more frequent, and their trajectory harder to predict, it is worth asking what current approaches are missing and what is still needed to address them. Performing large scale changes to already established critical infrastructure is unrealistic in the short term. Instead, implementing practical recommendations for managing and improving current systems is a more realistic approach. Achieving this requires both fundamental research and stakeholders confronting these issues and sharing what they have experienced.

On one hand, fundamental academic research provides a structured way to reason under uncertainty, compare options, weigh likely outcomes, and make trade-offs explicit, rather than relying only on instinct or on the loudest alarm. Research also makes it possible to test mitigation choices safely, including in simulation, before they are used in real operations. However, methods that look sound in models can fail in practice if they assume perfect data, ignore tool limits, overlook legacy constraints, or underestimate how decisions are made during stressful incidents. Research outputs can also be too specialized to translate into actions that mixed teams can apply quickly, across operations, security, and management. Stakeholders' experience fills the gap: it brings the real constraints on who can do what, in what order, under what rules and with what systems, and surface practical needs invisible to models, like what information operators trust, how alarms are handled, where handoffs break down, and what training is missing.

¹ D. E. Whitehead, K. Owens, D. Gammel, and J. Smith, "Ukraine cyber-induced power outage: Analysis and practical mitigation strategies", in *70th Annual Conference for Protective Relay Engineers (CPRE)*, 2017, pp. 1–8.

² D. U. Case, "Analysis of the cyber attack on the Ukrainian power grid", *Electricity information sharing and analysis center (E-ISAC)*, vol. 388, no. 1-29, p. 3, 2016.

³ Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and U.S. Department of Energy (DOE), "AA22-083A: Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector", *Cybersecurity Advisory*, online, Mar. 2022, last revised Mar. 24, 2022. Accessed: 2026-02-24. [Online]. Available: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-083a>

⁴ K. Proska, J. Wolfram, J. Wilson, D. Black, K. Lunden, D. K. Zafra, N. Brubaker, T. McLellan, and C. Sistrunk, "Sandworm disrupts power in Ukraine using a novel attack against operational technology", *Google Cloud Blog (Mandiant), Threat Intelligence*, Nov. 2023, published: Nov. 9, 2023. Accessed: 2026-02-24. [Online]. Available: <https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology>

⁵ ESET Research, "Industroyer2: Industroyer reloaded," *WeLiveSecurity (ESET) blog post*, Apr. 2022, published: Apr. 12, 2022. Accessed: 2026-02-24. [Online]. Available: <https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/>

⁶ NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), "Viasat KA-SAT attack (2022)," *International cyber law: interactive toolkit (Cyber Law Toolkit)*, wiki page, May 2022, last edited May 29, 2022. Accessed: 2026-02-24. [Online]. Available: [https://cyberlaw.ccdcoe.org/wiki/Viasat_KA-SAT_attack_\(2022\)](https://cyberlaw.ccdcoe.org/wiki/Viasat_KA-SAT_attack_(2022))

IEEE Power & Energy Magazine

Example Template for Draft Articles

This article gathers high-level recommendations targeting electric power system actors who collaborate with TSOs nourished through two main channels: (i) a corpus of fundamental research and (ii) the expertise of stakeholders who shared their views during a purposely organized series of workshops. After exposing the key points of each source of information, we synthesize essential recommendations, keeping them as non-technical as possible and understandable across roles, and we look for common denominators. Note that in this article, we choose to focus on the question of risk mitigation, even though it is often intertwined with the problem of risk assessment.

The rest of this paper is organized as follows: Section *Recommendations from fundamental academic research* proposes a recommendation-oriented synthesis of some recent academic research. Section *Recommendations from stakeholder's feedback* synthesizes the views of some stakeholders shared during the workshop series. Section *Discussion* and *Conclusions* discuss some common denominators between elements detailed in previous sections and conclude the paper.

Recommendations from fundamental academic research

We structure the research-based recommendations around three questions that map to where TSOs can make decisions in day-to-day operations: (1) Arbitrating between preventive and corrective cyber-physical risk mitigation, (2) Enhancing cyber-physical security in real-time operation, and (3) Enhancing cyber-physical security in look-ahead mode. These three questions align with three time horizons that drive most operational choices. Together, they form one connected story across the full operating cycle: ahead of time, before any incident, when preventive settings and operating margins are decided; in real time, during an incident, when the operator must keep the system stable with imperfect information; and in look-ahead planning, typically day-ahead, when dispatch and coordination decisions are prepared for the next operating period, often in an interconnected TSO context.

Arbitrating between preventive and corrective cyber-physical risk mitigation

The first research question to be explored is the extension to the domain of cyber-physical security of some classical methods mainly relying on multi-stage stochastic programming techniques and originating from the domain of physical security to the context of the arbitrage between preventive strategies and corrective strategies^{7,8}. 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 present context, preventive security management means taking decisions before any credible contingency event happens to ensure that the system can resist this event without any further intervention from its operator.

⁷ F. Capitanescu, J. M. Ramos, P. Panciatici, D. Kirschen, A. M. Marcolini, L. Platbrood, and L. Wehenkel, "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.

⁸ 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.

IEEE Power & Energy Magazine

Example Template for Draft Articles

From a more abstract perspective, a cyber sub-system can be represented as an interface between the physical grid processes and the system operator through two complementary variable vectors⁹: on the one side, operation-level interface variables perceived by the SCADA/EMS, and on the other side, field-level interface variables representing the actual physical state of equipment. From this abstraction, cyber-physical threats can be modelled as deviations from nominal interface values. A cyber countermeasure is a measure aiming for mitigating these deviations (e.g., setting the rules of existing firewalls, the thresholds for bad-data detectors, the topology of the communications network etc).

Unlike (stochastic) physical outage, cyber-threats are directed by independent decision makers, which results in a chain of 3 decision making processes: (1) an integrated cyber-physical planner (security manager), (2) a cyber-physical attacker, and (3) a real-time grid operator (see Figure 1). The interaction between these 3 actors can be formalized as nested tri-level optimization problem. The complexity of the resulting optimization problem depends on the level of information accessible to the attacker: while "perfect information" situations represent a theoretical worst-case scenario, real-world adversaries often operate with "imperfect information".

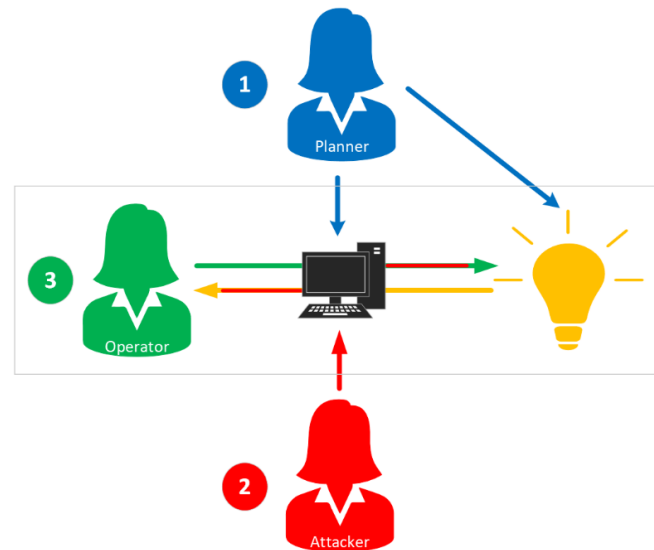


Figure 1: Sequence of decisions of cyber-physical security management.

From this research, our first key recommendation is *choosing the right scale*: there is a need to model the cyber sub-system of the power grid at a suitable level of detail considering 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 and the human operators (and control automata) of the power grid, has been introduced. Our second recommendation is *getting to know the enemies*: most relevant cyber-physical threats are not exogenous fatal contingencies, but rather intentional malicious attacks designed by intelligent agents who need to be described (motivations,

⁹ 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>

IEEE Power & Energy Magazine

Example Template for Draft Articles

resources, understanding and modelling skills regarding the cyber-physical electric power system). Our third recommendation is *managing mathematical and algorithmic complexity*: considering the two previous items when designing a decision-making framework, as it has been proposed by Karangelos and Wehenkel¹⁰ 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 exploring alternative decision-making approaches is recommended for future research.

Enhancing cyber-physical security in real-time operation

The question of improving real-time cyber-physical risk mitigation¹¹ naturally sits in the middle of the three research questions: once a cyber incident starts, decision-making shifts from choosing margins and settings to fast and effective actions taken with imperfect information, while still needing consistency with what was decided before and what will be planned next¹².

In practice, the real-time problem manifests in the control room as a credibility issue. Measurements may still arrive, but their meaning becomes uncertain. At the same time, some signals conflict, and parts of the supporting infrastructure may be degraded. Under these conditions, the operator's priority is not a complete root-cause story, but rapid containment and service preservation. It becomes critical to identify what can still be trusted, what can or must be isolated, keep essential functions running in a degraded mode if needed, and restore in an order that avoids secondary failures or a wider impact.

This is exactly where integrating diagnostic tools, anomaly detection mechanisms, and cyber-resilience approaches into real-time operation brings added value. Diagnostic agents can extract key features from both cyber and physical infrastructures and turn raw telemetry into usable situational awareness. Early identification of IT-OT anomalies can shorten time-to-detection and improve triage. Characterizing cyber-operators and the actions they can take makes response options realistic under time and resource constraints. Designing cyber-attack resilient cyber-physical systems targets continuity of critical functions even when the underlying infrastructure is partially compromised.

Taken together, these investigations highlight three practical needs in real-time operation: decisions must (i) account for cross-domain dependencies, (ii) remain actionable by operators under pressure, and (iii) work when the incident does not match a known script. These needs directly motivate the following recommendations. The first recommendation is *thinking in terms of the whole system and minding the interface*. This is important because attacks exploit interdependencies, so local actions must be evaluated

¹⁰ 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. 101872, 2025.

¹¹ L. Mathy, B. Knott, T. Behdadnia, D. Singelée, C. Ozkan, Z. Xinhai, and S. Kamyab, "Enhancing cyber-physical security in real-time operation," CYPRESS project, Tech. Rep., January 2025. [Online]. Available: <https://hdl.handle.net/2268/335745>

¹² S. Oshnoei, S. Hassani, M. Gheisarnejad, and E. Mahboubi-Moghaddam, "Real-time evaluation of cyberattack-resilient control for secure large-scale power networks", *IEEE Internet of Things Journal*, vol. 13, no. 3, pp. 4449–4462, 2026.

IEEE Power & Energy Magazine

Example Template for Draft Articles

for cross-effects. The second recommendation is *keeping the human in the loop*. This is essential because operators remain the key stabilizing element during incidents, which requires dedicated training and decision-support tools that remain reliable when conditions degrade. The third recommendation is *Thinking corrective strategies as adaptive and capable of generalization*. This matters because incidents do not follow a neat script, and better outcomes depend on real-time decision-making that can handle unforeseen behaviors, with IT, electrical engineering, and operations working together.

Enhancing cyber-physical security within look-ahead mode

A recently proposed approach for enhancing cyber-physical security in look-ahead consists in formalizing the problem through a day-ahead Cybersecurity Constrained Optimal Power Flow (CSC-OPF) framework¹³. This 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 minimize financial costs and lost load induced by the attack. The novelty of this approach 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.

Recently published¹⁴, this approach has been tested on two benchmarks: (i) two interconnected IEEE 39-bus using 3 transmission lines and (ii) two interconnected 118-bus test systems using 9 transmission lines. The attack scenarios focused on generator outages coming from compromised substations, where the attacker aims to maximize the product of attack success probabilities with their resulting physical impact (total load shedding). Simulations reach a zero-optimality gap in a few seconds (resp., a few minutes) for the 39-bus (resp., 118-bus) system benchmark. The iterative synchronization of inter-grid power exchanges requires an average of 29 (resp., 72) iterations for the 39-bus (resp., 118-bus) system. The decentralized model assumes TSOs only exchange average Value of Lost Load values once and perform iterative updates on inter-grid power exchanges. By decreasing shared data by 79.9% - 85.9% (depending on the system), the decentralized model improves privacy and autonomy. It remains close to optimality (with only a 0.4% - 0.6% cost gap) with a 0.3% - 4.7% risk increase compared to centralized coordination. It also achieves 12.3% - 18.9% total cost savings compared to non-coordinated planning.

¹³ 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>

¹⁴ A. Jafari, H. Ergun, and D. Van Hertem, "Risk-informed day-ahead cybersecurity enhancement planning in interconnected power systems: A decentralized privacy-oriented approach," Sustainable Energy, Grids and Networks, vol. 46, Art. no. 102279, 2026, doi: 10.1016/j.segan.2026.102279

IEEE Power & Energy Magazine

Example Template for Draft Articles

This research underlines the importance of *favoring decentralized coordination*. By avoiding 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. Another key recommendation is *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.

From planning to restoration: an end-to-end cyber-physical threat example

In this section, we connect the three research questions through one recurring cyber-physical threat scenario. The scenario is illustrative: it narratively connects the three academic questions by synthesizing outcomes from separate studies into a plausible storyline, rather than a single holistic simulation. The research articles^{14, 15} provide more detailed analyses within their respective domains.

The cycle begins in look-ahead mode. Consider an interconnected power system in which one control area is expected to rely on a highly loaded inter-area corridor. Before the next operating period, the TSOs prepare generation dispatch, inter-grid power exchanges, and corrective resources. Decentralized coordination limits the exchange of sensitive system information, while attack likelihoods help identify the cyber-physical events that should receive greater attention in the operating plan¹⁵.

The resulting plan then enters the preventive and corrective cyber-physical risk mitigation stage. By choosing the right scale, the planner represents the measurements, commands, communication services, and physical components most relevant to the secure operation of the corridor. Getting to know the threat actors helps identify which interfaces may be targeted, based on their possible knowledge, resources, and objectives. At the same time, managing mathematical and algorithmic complexity keeps the planner-attacker-operator problem detailed enough to support decision-making while remaining tractable for operational use. The result is a combination of preventive countermeasures and corrective resources made available to the real-time grid operator¹⁰.

During real-time operation, a cyber incident may affect the information exchanged between the field and the control center. Measurements may become incorrect, delayed, or unavailable, and an intended control command may not reach the relevant equipment. Diagnostic tools and anomaly detection mechanisms may provide an early indication of abnormal communication behavior, warning that some operation-level interface variables shown by the SCADA/EMS may no longer correspond to the field-level interface variables¹⁵.

If the condition persists, the control center may act on an incomplete or inaccurate view of the system. A planned generation adjustment may not take place, an inter-area transfer may rise above its expected

¹⁵ 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*, vol. 16, pp. 3305-3322, 2025.

IEEE Power & Energy Magazine

Example Template for Draft Articles

value, or a required control action may be delayed. The physical consequences may then appear as line overload, voltage deviation, active-power imbalance, or frequency deviation. If the violation remains unresolved, protection systems may operate and alter the network topology, possibly transferring stress to neighboring parts of the grid.

The early warning gives the operator time to compare the affected information with independent sources, restrict untrusted communication paths, and activate the corrective resources prepared earlier. Depending on the observed physical state, the operator may adjust inter-grid exchanges, redispatch generation, modify the grid topology, increase reactive-power support, or apply controlled load shedding. Since the actual incident may differ from the assumptions used during planning, the corrective response must remain adaptive while keeping the human operator in the loop.

Once the system has been stabilized, cyber-physical restoration begins. The actual field state is confirmed, affected devices and communication paths are checked, and measurement and control functions are gradually returned to service. The lessons obtained from the incident, including the effectiveness of preventive measures, detection mechanisms, operator actions, and corrective resources, are then fed back into the next look-ahead planning cycle. In this way, planning, prevention, real-time response, and restoration form a continuous loop in which each completed cycle improves preparation for the next operating period.

Recommendations from stakeholder's feedback

This section synthesizes the recommendations gathered through a workshop series specifically organized around the topic *Cyber-Physical Risk of the bulk Electric Energy Supply System: Enhancing Multilateral Co-responsibility*¹⁶. The primary objective of this event series was to capture industry perspectives and rules of good practice from actors of the Belgian bulk power system, spanning both regulated and non-regulated sectors across utilities, industrial players, and institutions. The consultation process followed a three-step structure combining hybrid (on-line and in-person at the University of Liège) and strictly in-person formats (at the University Foundation in Brussels). The first two hybrid sessions (gathering 26 and 31 participants, respectively) were dedicated to stakeholder presentations and interactive discussions aimed at identifying emerging risks and operational challenges. The third and final session (gathering 18 participants) served to present and refine the consolidated highlights synthesized by the research team from the preceding presentations and debates. In practice, the authors manually reviewed the material presented during the workshops, as well as panel discussions and questions raised by the attendees. The gathered elements (recurring concerns, challenges and good practices) were then synthesized into non-technical recommendations and shared back to workshop participants, both through email exchange and during the last workshop.

Perspective from the Belgian Federal Public Administration

¹⁶ Workshop series webpage: <https://sites.google.com/view/cypressworkshopseries/>

IEEE Power & Energy Magazine

Example Template for Draft Articles

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: (i) the energy transition, which started more than twenty years ago, (ii) the evolution of threat landscape, which has dramatically changed in the last three years¹⁷, and (iii) 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 defense 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 and iterative assessment procedures (see Figure 2). Belgium is collaborating both at the regional level (bilateral agreements, cross-border initiatives, North Sea Security Pact, North Seas Energy Cooperation¹⁸, at the European level (e.g., EU directives and recommendations, action plan on submarine cables), and within the North Atlantic Alliance.

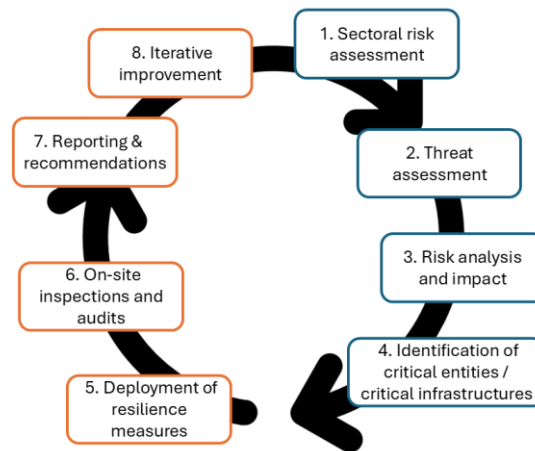


Figure 2: An iterative procedure for assessing and mitigating threats on critical infrastructure

The authorities expect from the operators a resilience capacity 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, 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.

¹⁷ See, for instance, the recent attack on a Norwegian dam:

<https://www.theguardian.com/world/2025/aug/14/russian-hackers-control-norwegian-dam-norway>

¹⁸ Link to The North Seas Energy Cooperation webpage:

https://energy.ec.europa.eu/topics/infrastructure/high-level-groups/north-seas-energy-cooperation_en

IEEE Power & Energy Magazine

Example Template for Draft Articles

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. This asks the question of how the legal framework should evolve to support the arrival 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). Opportunities are also related with new energy technologies for enhancing the resilience of the EU and the North Atlantic Alliance, 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 monitor the maritime domain (e.g., distributed acoustic systems, radars, cameras, sensors).

From the sharing of the Belgian Federal Administration, the following recommendation is emerging: *Strengthening collaboration between regulated and non-regulated sectors*. As energy networks 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.

Perspective from the side of TSOs

In this subsection, we chose to group the feedback from the Belgian TSO (Elia) with the one from 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. The perspective shared by the TSO has been structured along a list of seven points of attention, represented in Figure 3, and detailed below.

Firstly, digitalization transforms isolated substations into networked systems and offers new entry points for potential threats. Attackers can manipulate physical equipment using the Operational Technology (OT) of the energy infrastructure. Secondly, IoT communication (e.g., connected sensors) brings new vulnerabilities: attackers can perturb the observations, hide critical issues, potentially leading to the failure of the equipment to larger consequences. Thirdly, IT applications development cycles acceleration potential favors security gaps. One could imagine a manipulation of prices on the electricity markets leading to physical consequences, such as the hindering of renewable energy sources integration¹⁹. Fourthly, 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 emergencies to bypass crucial controls. Fifthly, new decentralized assets (solar PV, wind turbines, inverters, etc) introduce new risks: for instance, compromised offshore platforms could simultaneously disconnect GWs of power generation. Sixthly, emerging technologies (e.g., quantum computing, AI, autonomous systems, biometrics, edge computing) continuously reshape threat and defensive

¹⁹ 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.

IEEE Power & Energy Magazine

Example Template for Draft Articles

landscapes, often introducing black-box devices and software. In addition, some services may pose problems in terms of data sovereignty, for instance cloud storage. The use of non-EU solutions for storing or manipulating critical EU infrastructure data should be questioned. Seventhly, 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 incidents.

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

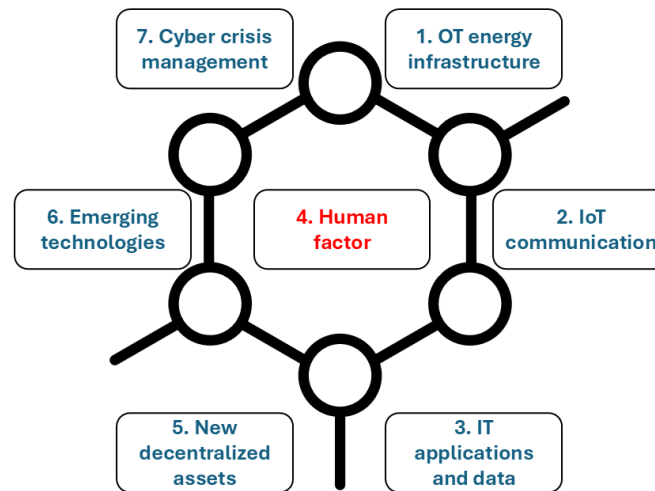


Figure 3: The TSO is at the crossroad of many sources of strengths and vulnerabilities.

A first emerging recommendation is *minding the 3D: data, digitalization and decentralization*. The process of digitalization in conjunction with the deployment of decentralized assets increases 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. A second recommendation is *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 concrete actions to help European TSOs move forward harmoniously²⁰. A third recommendation could be *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.

²⁰ See for instance, the TYNDP initiative which identifies gaps in infrastructure from a European perspective: <https://tyndp.entsoe.eu>

IEEE Power & Energy Magazine

Example Template for Draft Articles

Perspective from a DSO

DSOs share some common cyber-physical security challenges with TSOs. Distribution networks substations should be seen as cyber-physical systems, featuring different network activities: protection relays, intelligent electronic devices, remote terminal units and switches. Many physical security measures are already implemented, including airlock systems, video surveillance, intrusion detection systems, and environmental risks management.

DSOs have been concerned about building a resilient network for a while. Brussels' DSO (Sibelga), for instance, has operated its own optical fiber network since 2014 (nearly 280km), providing dedicated, telecom-independent, real-time remote-control to over 120 substation nodes. There is an automatic re-routing system in case of cable failure, and back-up batteries allow to maintain node power during blackouts.

There is a growing need for hybrid human skills encompassing both physical and cyber-physical awareness. Cyber-physical security should be considered as a collective effort, and part of this effort amounts to a cultural switch from thinking that it is an IT problem to realizing 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.

From this, a first recommendation is *working on change management and cultural switch*. Enhancing mitigation strategies for cyber-physical risks implies increasing staff competence and knowledge to extend safety culture to safety and cyber-physical security culture. A second recommendation is *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.

Perspective from services and technology providers

Through the different solutions they bring to the market, companies can both strengthen and undermine 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 reverse 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 assisting actors in assessing and enhancing their cyber-physical security. The design of a real-time cyber-physical simulator of the French network with the objectives to test new automata and train the operators is one such typical example

IEEE Power & Energy Magazine

Example Template for Draft Articles

provided by stakeholders. To do so, they rely on an information flow-based co-simulation approach²¹, which has the advantage of (i) requiring less data on the cyber-system, (ii) being computationally efficient, 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 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 for which transparent, open-source solutions are available to the public.

Discussion

Figure 4 synthesizes the recommendations from both academic and stakeholder channels. Three commonalities emerge. First, innovation is both the main vector introducing new cyber-physical threats and the main source of solutions to them, but using these new tools requires rigor in knowing their characteristics, potential and limits²². This is easier with open-source tools, even though openness brings its own risk of adversarial reverse engineering. Second, the human factor remains central to mitigating cyber-physical risk: the growing use of connected, potentially black-box hardware and software could itself become a threat unless paired with dedicated training or oriented toward human decision support, echoing both TSOs' focus on human factor strengths and vulnerabilities and DSO's call for change management and cultural switch. Third, decentralization and data management emerge as a shared concern: the research recommendation to favor decentralized coordination and smart data sharing in look-ahead planning parallels TSOs' attention to minding data, digitalization and decentralization.

Because cyber-physical simulation spans several system layers, timescales, and modelling assumptions, simulation and co-simulation tools remain an important area for further work²³. In the context of the three research questions addressed in this article, the required fidelity of the physical-layer model depends on the intended application. Steady-state models are generally suitable for look-ahead planning and for assessing preventive and corrective strategies. Electromechanical-transient models are needed when system dynamics and the real-time physical response to a cyber incident must be represented. Electromagnetic-transient models are required when fast control, protection, converter, or equipment behavior is central to the application.

²¹ Y. Cao, X. Shi, Y. Li, Y. Tan, M. Shahidepour, 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.

²² 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/>

²³ 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/>

IEEE Power & Energy Magazine

Example Template for Draft Articles

The required fidelity of the cyber and communication layers should follow the same principle. High-level models of data availability, integrity, delay, or command loss may be sufficient for planning and risk assessment, whereas packet-level or protocol-aware models may be needed when communication latency, congestion, routing, or attack propagation directly influence the physical response. For operator training and decision support, the main challenge is to represent the interaction between the cyber and physical layers with sufficient accuracy while preserving real-time execution and credible information flows, alarms, and response options. Such platforms should be validated at several levels, including comparison with accepted benchmark cases, trusted simulation tools, network or equipment measurements, and operational data where available. Review by system operators is also needed to confirm that the represented events, interfaces, decision times, and corrective actions are credible for practical use.

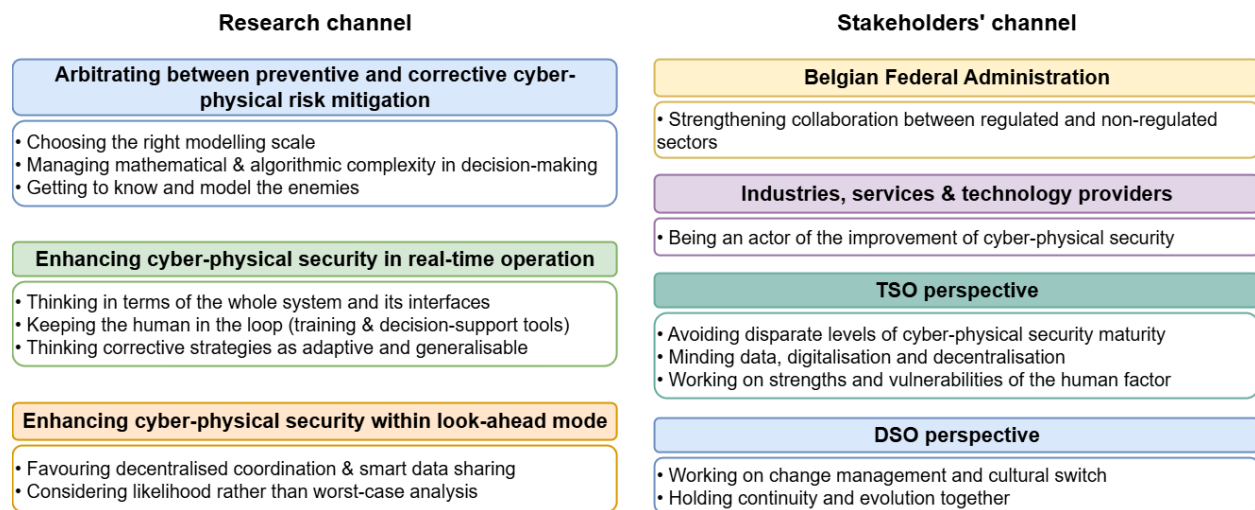


Figure 4: Synthesis of the recommendations coming out of the research and the stakeholders' perspectives.

Workshop panelists also discussed the idea of cyber-physical stress tests, drawing on the concept introduced after the 2008 banking crisis to assess financial institutions' resilience to adverse developments and to gauge systemic risk across the EU²⁴. Ongoing (co-)simulation developments can serve as building blocks for such a platform, though much academic and industrial work remains. Looking ahead, one panelist noted that any future research effort should give cyber-physical restoration a more central place, for instance through dedicated guidelines to coordinately restore both the physical power system and its most critical cyber-subsystems.

Conclusions

This article aims to aggregate recommendations from academia and stakeholders on the possibilities of mitigating cyber-physical risks of the electric power system, and ultimately to open prospects for future

²⁴ 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>

IEEE Power & Energy Magazine

Example Template for Draft Articles

developments. Recent work has demonstrated that it was possible to formalize and provide quantitative answers to research questions related to the assessment and the mitigation of cyber-physical risks. Indeed, access to data and real models for carrying out research 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.

Acknowledgments

This work has been prepared with the support of the Belgian Energy Transition Fund, project CYPRESS²⁵. Thanks to (in alphabetical order) Alireza Bahmanyar, Daiga Dege, Benjamin Krikler, Frédéric Olivier, Ludovic Rigaux, Frédéric Sabot, Loïc Tilman, Guillaume Van der Schueren and Annemie Vermeylen for sharing their expertise during the CYPRESS workshops. The responsibility of the content of this paper rests with its authors.

Biographies

Raphael Fonteneau and Louis Wehenkel are with the University of Liège, Liège, Belgium.

Tohid Behdadnia and Geert Deconinck are with KU Leuven, Leuven, Belgium.

Efthymios Karangelos is with the University College Dublin, Dublin, Ireland.

²⁵ <https://cypress-project.be/>