CYPRESS

Recommendations for determining cyber-physical risks and critical threats

Task 2.4 - Project Report

Pierre Henneaux, Can Özkan, Shahabeddin Kamyab

Date: November 2025

Table of Contents

1. Introduction

The ongoing energy transition is reshaping electric power systems into increasingly smarter infrastructures that take the form of cyber-physical systems. In these systems, electrical grids are deeply interwoven with advanced information and communication technologies (ICT), improving the observability and the controllability. While these capabilities are essential for ensuring the flexibility and reliability of future energy systems, they also expand the attack surface for cyber intrusions and introduce new forms of interdependencies between the cyber and physical domains. In response to these challenges, the CYPRESS[1] project aimed to develop comprehensive cyber-physical risk assessment and management frameworks for transmission systems. Cyber-physical risk refers to the combined likelihood and impact of events in which a cyber compromise propagates into the physical operation of the power system, causing measurable degradation of its reliability and/or resilience.

In order to reach its objectives, the CYPRESS project was articulated along three research work packages. The first work package developed criteria and benchmarks for cyber-physical risk management. The second work package, the focus of this white paper, developed techniques for assessing ex-ante the cyber-physical risks that could impact electric power systems. The third work package developed techniques to mitigate cyber-physical risks and to enhance the cyber-physical security of electric power systems. In addition to methodological advances, the CYPRESS project also conducted across the three work packages experimental case studies to validate the applicability of its frameworks to concrete infrastructures (such as transmission systems, distribution systems, wind farms, etc.).

Based on the outcomes of the second work package, this white paper provides recommendations to aid transmission operators in identifying relevant cyber-physical threats for their systems.

The remainder of this whiter paper is organized as follows. Section 2 reviews current practices in terms of cybersecurity risk assessment in Europe, and their expected evolution. On that basis, 3 emphasizes the main challenges that must be tackled to perform convincing cybersecurity risk assessments of real electric power systems. Section4 summarizes then the main contribution of the CYPRESS project to these challenges. Finally, Section 5 concludes by giving recommendations on the next steps.

2. Current practices and expected evolutions

At a worldwide level, several standards deal with cybersecurity risk assessment of industrial systems and critical infrastructures. Their scope encompasses thus electric power systems. They provide general guidelines to assess cybersecurity risks at system level. For instance, the standard IEC 62443-3-2 defines a risk assessment methodology for Industrial Automation and Control Systems (IACS) environments. In line with typical frameworks for risk assessment in general[2], the methodology consists in three main steps: identifying threats, estimating their likelihood and evaluating associated consequences. Additionally, it requires to identify and list countermeasures. Similarly, the NIST Cybersecurity Framework includes the identification of potential impacts and likelihoods of threats exploiting vulnerabilities.

In Europe, practices are expected to change in the upcoming years following the adoption by the European commission of the Network Code on CyberSecurity (NCCS) in 2024[3]. Although the NCCS focuses on cybersecurity aspects of cross-border electricity flows, its implications are broader than that. For instance, Article 18 requests the development of cybersecurity risk assessment methodologies at Union level, at regional level and at Member State level. Subsequent articles request regular risk assessments based on these methodologies.

[1] CYPRESS stands for “Cyber-Physical Risk of the Bulk Electric Energy Supply System” - https://cypress-project.be/

[2] I.e., not restricted to cybersecurity.

[3] Commission Delegated Regulation (EU) 2024/1366 of 11 March 2024 supplementing Regulation (EU) 2019/943 of the European Parliament and of the Council by establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows

In that context, all European TSOs proposed a first draft of cybersecurity risk assessment methodologies in November 2024, with the assistance of ENTSO-E and in cooperation with the EU DSO entity. Based on the public consultation, this draft has been revised and updated methodologies were formally approved by all TSOs on the 7th of March 2025. These methodologies are now submitted to national competent authorities for approbation. However, to the best of the authors' knowledge, at the moment of writing, the latest versions of these methodologies are not publicly available. Consequently, the discussion of this White Paper will be based on the versions published in November 2024.

Although the formulations for the methodologies at the three levels (Union, regional and Member State levels) slightly differ, the general philosophy behind them is the same. All methodologies rely on the same main steps: identification of threats, estimating their likelihood and evaluation of consequences. Regarding the first step, Annex III of the methodologies provide a generic list of threats that must be considered, at least for the regional cybersecurity risk assessment. On the contrary, no guide is provided to estimate their likelihood. Regarding the consequences, a list of impact metrics is provided in Annex I of the methodologies. This list comprises loss of load, reduction of power, frequency degradation, violation of standards on voltage, reduction of capacity in frequency reserves, loss of capacity for a black start, and the durations of customer interruptions. However, no guidance is provided on the approach(es) that should be used to evaluate these consequences, except that it should consider not only direct consequences but also indirect ones, for instance due to cascading effects.

The methodology for cybersecurity risk assessment at the Union level should be applied within 6 months of its approval. It is thus expected that it will become more concrete in the upcoming year.

3. Main challenges

Despite recent developments and progresses in methodologies to perform cybersecurity risk assessments, several challenges hampering their application to real electric power systems remain. These challenges are related to the typical three main steps of such methodologies:

- Regarding the identification of threats, the main challenge is related to the current lack of a comprehensive threat enumeration methodology in the ICS domain. Indeed, real electric power systems comprise many interconnected components, many of which are linked to ICT networks and therefore susceptible to cyberattacks. Identifying threats manually might be a daunting and impractical task due to the scale and diversity of components. There is a pressing need for systematic and automated techniques to efficiently and accurately identify threats across the system, which are currently lacking.
- Regarding the estimation of the likelihood of threats, we can first emphasize that there is no universally accepted methodology for quantitatively evaluating the likelihood of cyberattacks in this domain. Most risk assessment methodologies that have been developed in engineering (for instance to evaluate the reliability of a system) rely on statistics to evaluate the likelihood of the various sources of risk (e.g., failures). Such an approach does not seem relevant to estimate the likelihood of cyberattacks, because countermeasures are implemented after an attack occurs, significantly decreasing its future likelihood.
- Regarding the assessment of consequences, it remains unclear how specific threats can be translated into tangible consequences, such as the loss of supplied power. Although various methodologies have been proposed in the literature, there is no standardized approach for assessing the consequences of cyber threats on power systems. Furthermore, while European and international standards define general cybersecurity risk assessment procedures, very few explicitly consider renewable generation assets such as wind farms. The absence of domain-specific penetration testing exercises limits operators' ability to validate the effectiveness of risk assessment methodologies.

On top of that, we can also emphasize that existing works often focus on specific aspects of the overall cybersecurity risk assessment chain. The number of works proposing an integrated approach for the overall chain remains limited.

4. Contributions of the CYPRESS project

The CYPRESS project tackled these challenges and brought important contributions to close the gaps between academic literature and real-world needs. They are summarized hereafter with references to peer-reviewed papers and to deliverables of the second work package of the CYPRESS project[4].

Regarding the identification of threats, Özkan and Singelée proposed a novel threat enumeration methodology to systematically enumerate threats [1]. The proposed threat enumeration methodology is based on historical Common Vulnerabilities and Exposures (CVEs) entries of components and their associated Common Weakness Enumeration (CWE) entries in the form of CVE-CWE pairs. The applicability of the methodology is demonstrated on various Industrial Control Systems (ICSs) and on various associated components. This work offers significant advantages in enhancing threat identification, but it is limited to historical CVE and CWE values.

Regarding the estimation of the likelihood of threats, Jafari et al. proposed to improve traditional approaches based solely on the Common Vulnerability Scoring System (CVSS) through the consideration of sustained system access and of the dynamic nature of attack persistence [2]. For that purpose, they introduced a "persistence rate" in the computation of the likelihood of attack paths. Persistence rates are then estimated based on pre-persistence attack durations and mean times to reboot, such that the effects of system recovery cycles and prolonged attack duration are captured.

Regarding the assessment of consequences, the CYPRESS project brought various contributions both on the way to model cyber-physical power systems when they are enduring severe disturbances and on simulation methods. Not all of them will be mentioned here: but only the main relevant ones for this white paper. The reader is referred to the CYPRESS website for the other ones. A first contribution is related to the derivation of equivalents of active distribution networks for risk assessment at the level of transmission systems [3]. In that work, Sabot et al. proposed to derive equivalents based on quantiles of the behaviour of detailed models, to account for uncertainties. A second is related to the modelling of manual corrective actions that operators can take to mitigate a major disturbance [4]. In that work, Kamyab et al. proposed a Human Reliability Analysis-Optimal Power Flow (HRA-OPF) framework (i) to derive the optimal set of manual corrective actions that can be taken at each stage of the disturbance, but also (ii) to account for the fact that due to stressful and time-constrained situations, operators might not be able to take appropriate corrective actions in time and might even take counter-productive actions. A third contribution is related to the modelling of realistic cyber–physical attackers under imperfect information [5]. In that work, Karangelos and Wehenkel model load redistribution attacks aimed at inducing grid insecurity, while considering that such a malicious cyber-attacker would plausibly base its decision strategy on imperfect information. A fourth contribution focused on jamming attacks against remote-controlled switches during a fault detection, isolation and restoration process in a radial distribution system [6]. In that work, Bahrami and Wehenkel computed the probability of successful jamming attacks, load restoration times and Expected Energy Not Served (EENS) in different situations. Note that the estimation of the EENS is straightforward in that case as it results simply from a loss of connectivity. A fifth contribution focused on the impact of cyber-attack scenarios that target wind turbine stability by manipulating pitch angle and yaw control systems [7]. In that work, Özkan et al. implemented four attacks using both *pyModbusTCP* and *mbtget*, representing realistic adversarial behaviours. The study revealed that signature-based IDS solutions failed to detect these attacks, while Zeek's behavioural analysis identified anomalies. Furthermore, physical impact simulations showed that these cyberattacks could trigger transient instability and out-of-step conditions within seconds. A sixth contribution is related to the development of a co-simulation platform capable of simulating both the physical and cyber domains of power systems [8]. This platform relies on the open-source co-simulation framework HELICS to synchronize a time-domain power system simulator, Dynaωo, with an event-driven network simulator, OMNeT++. This synchronization ensures accurate modelling of interactions between the power and cyber domains. The platform has been developed up to the level of simulating the process bus, but future work is needed to extend it to the station bus and beyond, such that cyber-physical risk assessments can be based on a more complete model of cyber-physical interactions across all layers of the power system.

[4] Available on https://cypress-project.be/deliverables.

Finally, Jafari et al. proposed a comprehensive, realistic and practical framework for assessing cyber-attacks risks in power systems, integrating all the three steps (i.e., identification of threats, estimation of their likelihood and assessment of a consequences) in a single framework [2]. However, the application of the framework is currently limited to a very specific case study: cyber-attacks on frequency protection relays.

In a nutshell, the CYPRESS project brought important pieces of solutions to the main challenges emphasized in Section 3, as summarized in Table 1. However, additional work is needed to put all the pieces together to reach a comprehensive and convincing methodology for cybersecurity risk assessment.

Table 1: Overview of CYPRESS achievements and forward actions across the cyber-physical risk-assessment chain

Risk Assessment Step	Main Challenge (from Sec. 3)	CYPRESS Contribution	Reference / Deliverable	Main Remaining Gap / Next Step
Threat Identification	No automated or unified method to systematically identify and map cyber threats across industrial and power system components.	Evidence-based CVE–CWE pairing methodology to enumerate and classify vulnerabilities	Özkan & Singelée, 2025 [1]	Extend to *unknown* vulnerabilities via AI-assisted or ontology-based discovery methods
Likelihood Estimation	Lack of quantitative models to represent the evolving dynamics of cyber threats over time	Introduction of quantitative metrics to model how long attacks persist and how systems recover over time.	Jafari et al. (2025) [2]	Demonstrate scalability using realistic transmission-system data and integrate exposure and mitigation factors.
Consequence Assessment	Limited means to quantify system impacts of cyber events within realistic dynamic and operational contexts.	CYPRESS integrated multiple modelling tools to assess how cyber events affect the grid: (a) HRA-OPF for operator reliability, (b) a realistic attacker model under imperfect information, (c) a HELICS-based cyber-physical co-simulation, (d) a DPSA framework for dynamic impact quantification, and (e) a protocol-aware penetration-testing and detection setup on turbine-control attacks and resulting grid instability.	Kamyab et al., 2024 [4]; Karangelos & Wehenkel 2022 [5]; Ben Mariem et al., 2024 [8]; Sabot et al., 2023 [3]; Özkan et al., 2025 [7].	Extend co-simulation to higher system layers and establish unified indicators for dynamic impact and resilience assessment.
Integrated Framework	Lack of an integrated approach connecting threat, likelihood, and consequence analysis.	Prototype integrated framework uniting all stages of the cyber-risk assessment chain.	Jafari et al. (2025) [2]	Validate on large-scale system cases and align with NCCS risk assessment approaches.

5. Conclusions and recommendations

Cybersecurity risk assessment in modern electric power systems remains a complex and evolving challenge. Despite the abundance of research in this domain, there is still no comprehensive and convincing methodology that effectively addresses all aspects of the problem. This gap underscores the need for more robust and pragmatic approaches that can be applied in real-world scenarios and produce actionable insights.

One of the primary difficulties lies in the identification of threats. Given the vast number of components in electric power systems and their increasing integration with ICT networks, many elements are potentially vulnerable to cyberattacks. However, it is impossible to be exhaustive in identifying all threats, especially when unknown vulnerabilities may exist. Manual identification is impractical for large real power systems, which calls for the development of systematic and automated techniques to support this process. The CYPRESS project progressed in that direction, but the methodology developed so far rely on historical CVE and CWE analysis. The identification of threats that are not known yet or publicly documented is thus limited. Further work is thus needed to expand the scope of that methodology, such that cyber threats can be identified in an exhaustive and systematic manner, including threats propagating from systems external to the one under consideration (e.g., threats coming from distribution systems or from generating units when the risk assessment deals with the transmission system).

Evaluating the likelihood of cyberattacks presents another major obstacle. Traditional statistical methods are often irrelevant because countermeasures are typically implemented after an attack occurs, altering the conditions and making historical data unreliable. Moreover, precise likelihood estimation often depends on expert judgment, which introduces subjectivity and variability. The CYPRESS project enhanced existing methods to estimate the likelihood of threats. The scalability of these enhanced methods to large power systems and their applicability to real power systems remain however to be demonstrated.

Similarly, assessing the consequences of cyber threats is quite complex. The CYPRESS project proposed improvements in models and in tools that can be used for that purpose. However, attempting to estimate very accurately all possible consequences through over-elaborated models and simulation tools appears to be unrealistic for real power systems due to the immense computational resources and data required. Consequently, the good trade-offs between accuracy and feasibility must be found.

To overcome the remaining challenges and to put the pieces of the puzzle together, fostering collaboration between academia and industry/utilities is essential. Such partnerships can help direct research efforts toward the most pressing issues and ensure that theoretical advancements are grounded in practical needs. By working together, stakeholders can develop more effective cybersecurity risk assessment methodologies that are both scientifically sound and operationally viable. At the European level, the authors advocate to associate the academic sector to the implementation of cybersecurity risk assessment methodologies, for instance by including universities in the list of entities that should be represented in the Cybersecurity European Stakeholder Committee, or by creating a dedicated consultative group for the implementation of cybersecurity risk assessment methodologies including academia (as it was done for the latest bidding zone review). Furthermore, advancing cyber-physical risk assessment requires secure and well-structured data sharing between utilities and research institutions. Indeed, calibrating probabilistic models and validating simulation results depend on access to realistic operational and cybersecurity data, such as system measurements, protection logs, and anonymized incident records. In practice, however, this information often remains confined within utilities because of confidentiality and regulatory restrictions. Consequently, the authors advocate for the development of data-sharing practices to help researchers develop models that better reflect how real systems behave, while giving utilities a way to verify and improve their protection measures.

Associated publications of the CYPRESS project

[1] C. Özkan et D. Singelée, «A Novel Evidence-Based Threat Enumeration Methodology for ICS,» chez *Proceedings of the 40th IFIP International Conference, SEC 2025*, Maribor, Slovenia, May 2025.

[2] A. Jafari, C. Özkan, H. Ergun, D. Van Hertem et D. Singelée, «An advanced cybersecurity risk assessment framework: Integrating vulnerabilities and exploitation techniques for systematic attack path analysis in multilayered power system networks,» *Sustainable Energy, Grids and Networks,* vol. 43, 2025.

[3] F. Sabot, P. Henneaux, I. S. Lamprianidou et P. N. Papadopoulos, «Statistics-informed bounds for active distribution network equivalents subject to large disturbances,» chez *Proceedings of the 2023 IEEE PES Innovative Smart Grid Technologies Europe (ISGT EUROPE)*, Grenoble, France, Oct 2023.

[4] S. Kamyab, P. Henneaux et P.-E. Labeau, «Modeling manual corrective actions in probabilistic risk assessment of cascading outages,» *Electric Power Systems Research,* vol. 234, Sep 2024.

[5] E. Karangelos et L. Wehenkel, «Cyber–physical risk modeling with imperfect cyber-attackers,» *Electric Power Systems Research,* vol. 211, Oct 2022.

[6] M. Bahrami et L. Wehenkel, «A stochastic Petri net model of jamming attacks on remote-controlled switches during service restoration,» chez *Proceedings of the 2025 IEEE Kiel PowerTech Conference*, Kiel, Germany, Jun. 2025.

[7] C. Özkan, D. Singelée, A. Jafari Arnajan, R. Loenders et H. Ergun, «Penetration Testing in Wind Farms: Detection and Impact Analysis,» chez *Proceedings of the IEEE PES ISGT (Innovative Smart Grid Technologies) Europe 2025*, Malta, Oct. 2025.

[8] S. Ben Mariem, A. Leerschool, A. Godfraind, A. Bahmanyar et L. Duchesne, «CYPRESS D2.2 - Co-simulation of cyber-physical transmission systems,» 2024.