

# Πυλώνες 2 Pylons

Ηλεκτρονικό Περιοδικό  
Ελληνικής Επιτροπής CIGRE

e-Magazine  
CIGRE Greece NC

ΑΦΙΕΡΩΜΑ

*Αβεβαιότητα*

*Ασφάλεια*

*Ανθεκτικότητα*

SPECIAL ISSUE

*Uncertainty*


*Security*


*Resilience*

Απρίλιος 2022

April 2022

# Towards cyber-physical security for the electric power system

by  Efthymios Karangelos ✉  
Montefiore Institute - University of Liège

 Louis Wehenkel ✉  
Montefiore Institute - University of Liège

## — The cyber-physical electric power system

The continuous operation of large-scale electric power systems is a most complex achievement integrating technical, economical and organizational considerations. In addition to a well-functioning physical infrastructure (generators, transformers, lines, substations, etc.) it relies on a well-functioning cyber infrastructure, consisting of both hardware (sensors, smart meters, digital protection and control devices, communication routers and switches, data storage servers, etc.) and software (market clearing algorithms, supervisory control and data acquisition systems, billing and settlement tools, home energy management tools, etc.). Such hardware and software is embedded within all physical domains and hierarchical zones of the system, so as to enable their interoperability across several functional layers, as depicted by Figure 1.

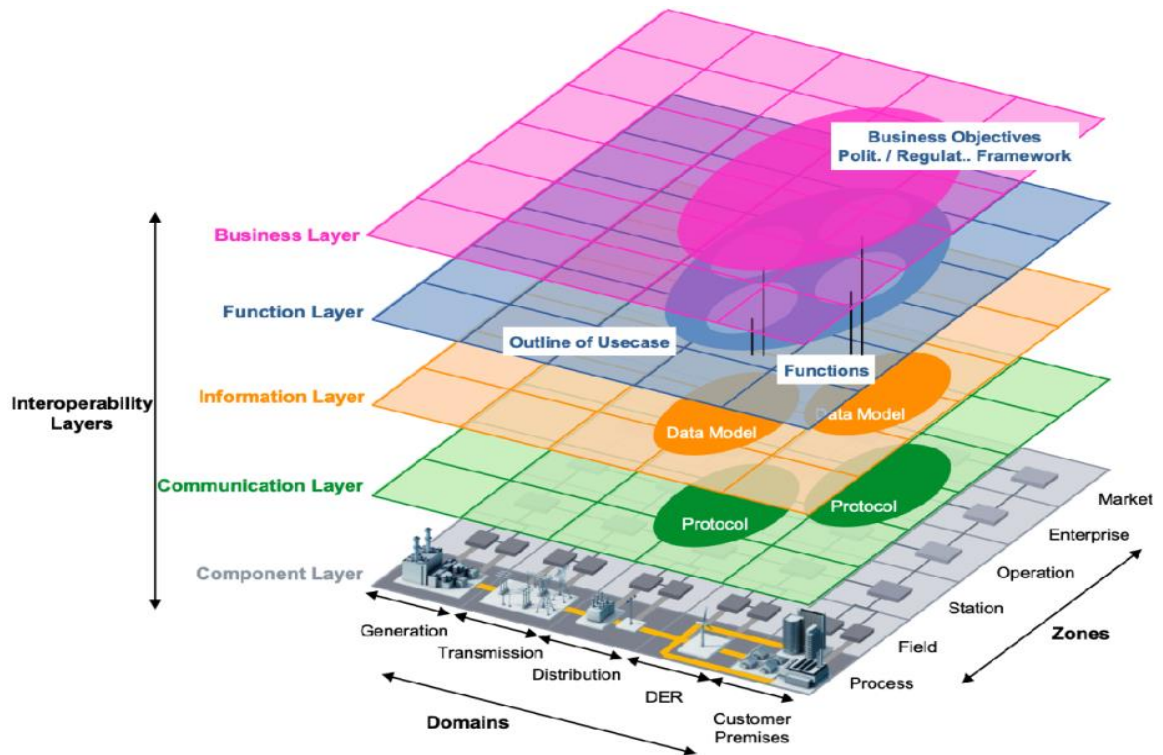


Figure 1 The Smart Grid Architecture Model (Smart Grid Coordination Group 2012)

## The essential functionalities of cyber infrastructure

While the term *Smart Grid* became popular at the start of the 21st century, the planning, operation and control of the electric power system has long ago been facilitated by *Information, Communication and Operational Technologies (ICT and OT respectively)*. Indeed, metering, control, communication and computational solutions were already in place well before the end of 20<sup>th</sup> century to achieve both technical reliability and economic efficiency, indicatively:

- The *Energy Management System/Supervisory Control and Data Acquisition (EMS/SCADA)* providing the transmission-level control center with key functionalities such as state-estimation, contingency analysis, automatic generation/voltage control and remote generation dispatching.
- The *Substation Automation System (SAS)* providing functionalities of data acquisition, remote and local control at the substation level (and connected assets) by combining *Remote Terminal Units (RTUs)* for communication, *Programmable Logical Controllers (PLCs)* for rule-based control implementation, *Protection Relays* to operate circuit breakers, *Metering and Monitoring Devices* as well as local *Human Machine Interfaces (HMIs)*.
- The *Generation Management System (GMS)*, providing functionalities to monitor, control and optimize the performance of power generation assets while also interfacing with the electricity market.
- *Advanced Metering Infrastructure (AMI)*, providing measurements of the end-consumer demand to electric utilities and pricing information to end-consumers in finer temporal resolution, allowing both to optimize their engagements with the electricity market.
- *System Protection Schemes (SPS)*, automatically triggering predetermined control actions to preserve the system stability and integrity, upon detecting the fulfilment of a specific condition in terms of measured electrical variables.

## The low-carbon transition will be digitally-enabled

In the present times, electric power systems are undergoing a fundamental transformation to keep up with the modern environmental, economic and technical developments. The combined effect of such developments will be pushing the physical infrastructure closer to its limits, and the foreseen transformation can only be completed with enhanced support from the cyber infrastructure. The future electric power system will be shaped by environmental, economic and technical considerations and enabled by an evolving cyber infrastructure.

On the environmental front, the ambition to mitigate climate change through the decarbonization of the energy sector is translated in concrete goals concerning electric power systems and more broadly the sourcing of energy to facilitate societal activity. These goals combine into major technical challenges as future electric power systems shall operate with a larger share of renewable generation while simultaneously carrying a larger share of the overall energy

supply. Tackling the natural variability, stochasticity and dispersed nature of renewable electricity generation with advanced forecasting techniques, exploiting more data and stronger computational resources, can only be achieved at a certain extent. It would have to be combined with a wider adoption of automated SPS to combat the increased variability of the generation sub-system by responding automatically to the detection of undesirable/insecure system states<sup>13</sup>, faster and more efficient security analysis tools to maintain operator situational awareness as well as advanced decision-making aids to navigate the power system under lower visibility. At the same time, whilst aiming to mitigate climate change, the system remains exposed to its adverse effects, such as more frequent and more extreme weather events. Helping the physical system deteriorate mildly and recover gracefully from such events (outside the scope of day-to-day security management) also necessitates enhanced monitoring, control, communication and computation capabilities.

On the economic front, the growing penetration of volatile, zero-marginal cost weather driven generation requires efficiently managing the implied financial risks of various stakeholders. The main foreseeable institutional instruments to do so are (i) the wider integration of regional electricity markets through increased interconnection capacity, (ii) bringing the market gate closure closer to the moment of delivery and (iii) enlisting the active participation of end-consumers even at lower voltage levels. The former two options challenge the current planning and operational practices of *Transmission System Operators (TSOs)* facing the mission of cooperating over larger geographical areas while having less time to decide (and/or more uncertainty). Maintaining the same security level seems therefore credible only by also enhancing the communication and computational tools in place towards more direct inter-TSO coordination. Further, the active participation of end-consumers in the electricity market (either at the wholesale level by means of aggregators, or through novel market structures at the level of energy communities) brings forward the issue of revamping the cyber infrastructure for active distribution network management. Further, extending the coordination between TSOs and *Distribution System Operators (DSOs)* for the provision of ancillary services, reserve and balancing products requires additional ICT infrastructure both for the aggregation of the products and services available downstream from the distribution feeder and for the efficient operation of these (novel) markets.

On the technical front, the existing physical infrastructure is ageing whilst new technologies are evolving towards maturity. The ageing of the physical infrastructure brings more relevance to advanced computational solutions for conditional-based maintenance, through the further deployment of measurement and communications hardware, and inevitably increases the complexity of the outage planning problem. On the other hand, the growing penetration of renewable generation resources is reducing system inertia, calling for the increased use of wide area controls and communications to coordinate the provision of fast frequency response by distributed resources (including storage

---

<sup>13</sup> Indeed, with increased variability the available time to detect and react shortens and preparing event-based controls against all possible events becomes unattainable. Response-based control offered by SPS circumvents these challenges by automatically applying “universal” remedial actions upon detecting an unwanted/insecure condition of the system electrical state.

devices and flexible loads). The call for wide(r) area controls, secure and fast(er) communications is amplified by the increasing usage of innovative transmission technologies such as *High Voltage Direct Current (HVDC)* interconnectors and controllable *Flexible Alternating Current Transmission Systems (FACTS)*. At the same time, at the distribution-level of the system, new technologies such as home energy management, energy storage and notably inverted-based distributed energy generation are progressively being adopted by end-users *en masse*, thus significantly enlarging the scale of the electric power system cyber infrastructure. Last but not the least, algorithmic progresses, such as the recent advancements in Machine Learning and in its applications to power systems (L. Duchense 2020), enlarge the possibilities for faster and more robust software applications.

## — Cyber-physical threats & countermeasures

Power system security management is predominantly focused on tackling physical threats to the electricity supply (e.g., the potential forced outages of the physical system components). The growing reliance on the system cyber infrastructure brings into the spotlight an additional class of threats, namely cyber-physical threats. Cyber-physical threats are malfunctions of the cyber infrastructure adversely affecting the operation of the physical system. Most alarmingly, in the case of cyber-physical attacks, a malicious entity may seek to compromise the cyber infrastructure functionality with the final aim of disrupting the supply of electricity.

The potential to launch successful cyber-physical attacks against the electric power system has been long-ago demonstrated experimentally. Back in 2007, the *Idaho National Lab (INL)* successfully performed a so-called *AURORA ("Avoiding Unwanted Reclosing on Rotating Apparatus")* cyber-physical attack against a diesel generator. In this attack scheme, the malicious actor takes control of the generator circuit breaker and issues a sequence of open and close commands, in a faster timeframe than the generator protection. These commands progressively desynchronize the generator from the grid, while the reclosure of the circuit breaker when the generator is out-of-phase produces great torque and electrical stress (Potvin 2019). As seen in a [video](#) recorded during the INL experiment, such an attack can finally cause permanent physical damage to the generator.

### Real-life cyber-physical attack experiences

Unfortunately, the potential of a successful cyber-physical attack has also been validated in practice. In two separate incidents, cyber-attackers have managed to disrupt the functionality of the Ukrainian electric power system. First, in the most significant event of December 2015, around 225000 customers suffered an interruption of about 6 hours in the Kiev district (J.E. Sullivan 2017). This attack targeted the local distribution network and featured an elaborate combination of social engineering to gain access, malicious software to manipulate the system as well as attacks on communications to compromise the diagnosis of the situation and also delay the restoration process. The cyber-attackers successfully took control of the SCADA system and remotely opened several circuit breakers, removing distribution substations from service. The attackers also

deprived control centers of back-up power, flooded the communication network with additional traffic and finally installed compromising software at the field devices, making it much harder to re-energize the affected substations.

The second event took place in December 2016, and this time targeted the Ukrainian transmission system (Slowik 2019). While it resulted in a less severe disruption, with a reported interruption of an hour in the city of Kiev, evidence suggests that it was designed to cause more severe physical damage to the system infrastructure. Once again, the central step of the cyber-physical attack was the hijacking of the SCADA system, allowing attackers to remotely control circuit breakers and switches. Ex -post analysis revealed that the attackers also attempted to deactivate protective relays on the transmission lines that were disconnected from the grid during the initial attack phase. Once re-energized by the system operators, these unprotected transmission lines could lead to a more severe system failure. This unwanted situation has been avoided thanks to the ability of the grid operators to manually reclose the attacked circuit breakers in short time.

As reported by the *North American Energy Reliability Corporation* (NERC 2019), the US grid also fell victim to malicious cyber-attackers in March of 2019. The intrusion became possible due to a known vulnerability of a firewall system and allowed the cyber-attackers to deprive the control center operators of their situational awareness for a brief time period. This was achieved by compromising the communication between the control center and remote field devices. Fortunately, this brief incident was mitigated without any impact on the functionality of the physical system. Finally, at the time of writing, there is still [speculation](#) whether the 2020 Indian blackout was the result of a cyber-physical threat.

### Taxonomy of cyber-physical threats

Comprehensively describing a cyber-physical threat amounts to defining the *adversary* (in terms of its role and motivation), its *resources* (in terms of computational capabilities and knowledge of the cyber and physical infrastructure) and its *strategy* (in terms of gaining & maintaining access through the cyber infrastructure and compromising it to affect the system functionality).

Table 1 presents a standard classification of adversary roles and motivations. Notice that this also includes so-called “careless or poorly trained employees”, that may unwillingly behave as an adversary.

*Table 1 Adversary Roles and Motivations (The Smart Grid Cybersecurity Committee 2014)*

<b>Nation States</b>	State-run, well organized and financed. Use foreign service agents to gather classified or critical information from countries viewed as hostile.
<b>Hackers</b>	A group of individuals (e.g., hackers, crackers, trashers, and pirates) who attack networks and systems seeking to exploit the vulnerabilities

	in operating systems or other flaws.
<b>Terrorists/ Cyberterrorists</b>	Individuals or groups operating domestically or internationally who represent various terrorist or extremist groups.
<b>Organized Crime</b>	Coordinated criminal activities including gambling, racketeering, narcotics trafficking, and many others. An organized and well-financed criminal organization.
<b>Other Criminal Elements</b>	Another facet of the criminal community, which is normally not well organized or financed. Normally consists of few individuals, or of one individual acting alone.
<b>Industrial Competitors</b>	Foreign and domestic corporations operating in a competitive market and often engaged in the illegal gathering of information from competitors or foreign governments in the form of corporate espionage.
<b>Disgruntled Employees</b>	Angry, dissatisfied individuals with the potential to inflict harm on the smart grid network or related systems.
<b>Careless or Poorly Trained Employees</b>	Users who, either through lack of training, lack of concern, or lack of attentiveness pose a threat to smart grid systems.

Defining the resources of an unknown adversary is arguably a non-trivial task. A commonly used risk averse approach is to focus on the worst-case threat posed by a computationally powerful and knowledgeable adversary that has performed diligent reconnaissance. It is however well relevant to also migrate from these worst-case assumptions and consider alternative cyber-physical threats, differentiated by the adversary's computational capabilities and level of system knowledge. In fact, game-theoretic analysis of the defender vs cyber-attacker interaction suggests that preparing to face a fully rational attacker with perfect knowledge is not the best strategy for protecting the electric power system (A. Sanjab 2016). Such a strategy leaves the system well exposed to the alternative attack strategies launched by realistic cyber-attackers with bounded rationality. Further, research works have shown that an adversary does not need complete or fully correct knowledge of the power grid to launch a successful cyber-physical attack (M. A. Rahman 2012, J. Zhang 2018). Considering realistic adversaries with imperfect information and/or limited computational resources is therefore a necessary complement to the worst-case approach for cyber-physical security (E. Karangelos 2022).

The broad spectrum of known strategies (H. He 2016) can be synthesized based on the compromised functionality of the cyber infrastructure initiating the threat sequence. *Measurement* based attack strategies compromise the integrity of information so as to induce erroneous operation of automated control loops and/or deceive the system operators into performing erroneous actions or missing alerts. For instance, tampering with the measurements involved in the *Area Control Error (ACE)* computation can eventually destabilize the electric power system, in AGC attacks. In so-called load redistribution attacks, the strategy is to present false load data to the system operators, provoking misguided reactions to cause economic efficiency losses and/or physical security violations. The previously introduced Aurora attack falls in the category of *control signal* based strategies while the incident of March 2019 is an example of a *data availability* based strategy. In practice, as evidenced in the Ukrainian experience, realistic cyber-physical threats are most elaborate and integrate measurement, data availability and control signal based strategies.

## Countermeasures for cyber-physical security

Countermeasures against the cyber-physical threats serve the functions of *protection, detection and mitigation*.

Protection counter-measures can be used at the level of individual field devices, sub-systems of the cyber-infrastructure as well as the integrated cyber-physical system. At the level of field devices, security and encryption techniques are used to protect the integrity of selected critical measurements thus making the system immune to *false data injection* attacks. Selecting such critical measurements requires assessing the system vulnerability against a defined set of credible cyber-physical threats. Firewalls are a well-established tool to block potentially harmful incoming traffic, while the use of encryption techniques is essential for ensuring the integrity and confidentiality of the communications network (i.e., at the level of a sub-system of the cyber infrastructure). An interesting protection countermeasure at the level of the integrated cyber-physical system consists of preserving the confidentiality of the cyber and/or physical infrastructure properties (e.g., the topological information of the transmission grid). Indeed, depriving potential adversaries of the information required to design a successful cyber-physical attack strategy effectively protects the integrated system from such a threat. The concept of *moving target defense* involves frequent, relatively minor adaptations of the system configuration so as to compromise the knowledge of a potential adversary.

Detection countermeasures are a necessary complement, since it is naturally impossible to successfully protect the system from the very vast range of potential cyber-physical threats. The so-called *Intrusion Detection Schemes (IDSs)* in place at the cyber infrastructure level are either signature based or anomaly based. Signature based schemes rely on physical watermarking, i.e. injecting a known noise on top of an input signal so as to produce a predictable output, for verifying the integrity of communications. Anomaly based schemes monitor the network traffic and rely on filtering techniques (and, more recently advanced *Artificial Intelligence & Machine Learning* tools) to identify and flag suspicious traffic patterns, suspected false and/or bad data. Further, model-based detection can also be applied at the level of the integrated cyber-physical system. Model-based schemes rely on simulating the estimated evolution of the physical system (e.g., near real-time, look-ahead power flow analysis) so as to identify suspicious deviations in the data coming through the cyber sub-system.

While all aforementioned detection countermeasures are useful, detecting an unwanted event does not stop it from compromising the cyber-physical system. At the cyber sub-system level, mitigation tools can be used to promptly restore the integrity, confidentiality and integrity of information. Specifically, pushback methods block incoming traffic from possibly compromised nodes of the communication network and reconfiguration methods remove possibly compromised network nodes. Mitigation is a most challenging task at the cyber-physical system level especially since realistic cyber-attacks involve several stages and integrate several sub-strategies. The [\*Rapid Attack Detection, Isolation and Characterisation Systems \(RADICS\)\*](#) program recently developed a suit of new technologies, including tools for restoring the situational awareness of control centre operators as well as for securing communications and



coordination channels in a post-attack stage. Most interestingly, several [live field-tests](#) were performed in the framework of this program simulating cyber-physical attack scenarios on an islanded micro-grid and developing methods for black start recovery in post-attack.

## — The stage for research & development

The ongoing modernization of the electric power system, along with the recent materialization of cyber-threats (also targeting other critical infrastructures and societal activities), set the stage for more intensive research and development towards cyber-physical security management for electric power systems. Addressing such research questions requires joint effort between the power systems and computer engineering communities, to progressively develop shared power-systems cyber-physical expertise.

### Modeling for cyber-physical security

Recent research efforts have achieved considerable progress on modeling the cyber-physical behavior of the electric power system. Merging models of the system cyber and physical infrastructure into a centralized, integrated simulation approach is arguably a complex technical task. The alternative of co-simulation, that is coupling modular models of the different sub-systems and functions in a distributed style offers advantages both in terms of efficiency and in terms of flexibility. Co-simulation can be leveraged to fine-tune the modeling granularity (in terms of time, space, etc.) independently for each sub-system, to re-use/recycle and upgrade available models of the different sub-systems, to parallelize computations while engaging specific solvers for different computational parts and to profit from domain-specific knowledge on the different fields. Notably, it also allows to rely on hybrid simulation architectures, wherein mixtures of software and hardware are used to represent the interaction between the system cyber and physical infrastructure. As an example<sup>14</sup>, Figure 2 illustrates the functional architecture of the so-called [Smart City](#) co-simulation environment developed at the *Washington State University*. This environment combines hardware of the physical and cyber systems (e.g., solar panels, smart meters, protection relays, EMS/SCADA etc.) with software simulators of the communication network and the power grid.

---

<sup>14</sup> A survey of cyber-physical electric power system co-simulation efforts can be found in (I. Zografopoulos 2021).

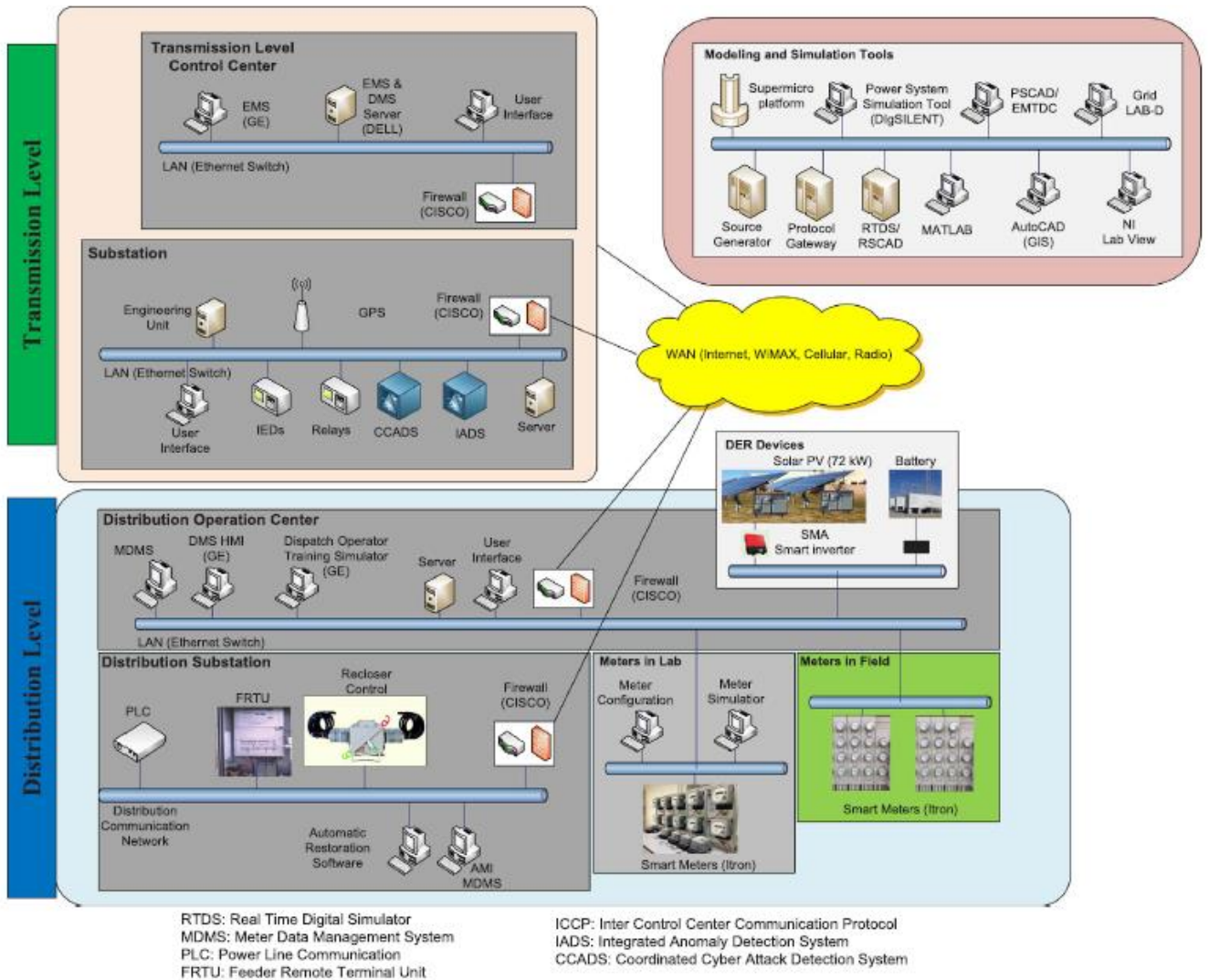


Figure 2 The Smart City Test-bed Architecture (CC Sun 2018)

The evolving role of the cyber infrastructure poses further questions for research and development, at the same time as the cyber-physical modeling field is progressing. Currently, the growing population of cyber hardware (e.g., power electronics inverters, smart meters) and software (e.g., battery management systems) at the end-consumer edges of the system reframes the question of bulk power system modeling. Specifically, as “passive” distribution networks are transforming into “active” cyber-physical sub-systems, there is a need to revisit their equivalent modeling approaches so as to capture both their cyber and physical behavior in an efficient and meaningful way. A similar open question can be stated at an “horizontal” level, that is when using equivalent models to represent the behavior of neighboring transmission control areas in single-TSO centric system models.

## Cyber-physical security assessment

‘Traditional’ methods and tools for physical security assessment have been managing the scale of the problem thanks (in part) to the favorable statistical properties of physical failures. As per the N-1 criterion for instance, the set of credible outages taken into consideration is a much smaller subset of the set of system component groupings. This practice is based on the statistical confidence that the likelihood of all other discarded failures and outages is small enough to render their expected impact negligible. Conversely, the cyber-physical threat surface is even broader and the statistical data and information necessary to reason on the relative likelihood of different threats is mostly unavailable. At the same time, non-malicious cyber-physical threats may simultaneously affect a large population of components while malicious cyber-physical threats may be developed over several stages (from an initial disruption to further barriers compromising the ability to restore the system back to full service). There is therefore a need to tackle computational complexity in order to be able to compute credible security indicators. Beyond the computational complexity of using software to simulate a single instance of the cyber-physical system operation, further research can be targeted towards developing efficient assessment methods to navigate the broad threat surface. Last but certainly not the least, meaningful criteria to translate the outcome of (massive) simulations into usable and informative electric power system cyber-physical security indicators need to be developed.

## Cyber-physical security management

Cyber-physical security management methods and tools are presently a ‘holy grail’ for research and development for electric power systems. One must first notice that the current state-of-the-art approaches for physical security management (increasingly) rely on a well-functioning cyber infrastructure to provide the necessary situation awareness (through measurements, communications, data storage and computations) and to facilitate the implementation of open-loop and closed-loop, manual and automated controls. The class of non-malicious cyber-physical threats already challenges these approaches and it appears impossible to ensure the same level of security without the functionalities provided by the cyber infrastructure. Progress on cyber-physical threat detection techniques brings into the spotlight the question of how to operate the electric power system once its cyber infrastructure is known to be compromised. By now, it is well understood that achieving full immunity against all possible cyber-attacks is both technically unreachable and economically inefficient. There is however only moderate progress on finding a middle ground between full immunity and the happy-go-lucky alternative of neglecting cyber-physical threats. While considerable research and development efforts have already provided solutions for protecting against, detecting and mitigating specific cyber-physical threats, a holistic approach facing a spectrum of potential alternative threats is needed in practice. It must further be compatible/combined with the current, physical-focused security management approach, in a way that maintains at a suitable level the overall security of the electric power system.

## The CYPRESS project

These research and development challenges form the background for the [Cyber-Physical Risk of the bulk Electric Energy Supply System \(CYPRESS\)](#) research project. The CYPRESS project aims at developing novel knowledge, methods and tools needed to help ensuring the security of supply through the transmission grid, while accounting for the specific nature of cyber-threats and integrating them into a coherent probabilistic risk management approach. The project started 1 November 2020 and will last 5 years, with the support of the Belgian Energy Transition Fund. The project consortium brings together electrical power systems and computer engineering experts from three Belgian Universities, namely *Université de Liège* (also in the role of project coordinator), *Katholieke Universiteit Leuven* and *Université Libre de Bruxelles* and an industry leader in the field of IT solutions for electric power systems, *Haulogy*.

## Acknowledgment

This publication has been prepared with the support of the Belgian Energy Transition Fund, project CYPRESS (<https://cypress-project.be>). The opinions expressed are those of the authors.

## — References

- A. Sanjab, W. Saad. 2016. "Data injection attacks on smart grids with multiple adversaries: A game-theoretic perspective." *IEEE Transactions on Smart Grid* 2038-2049.
- CC Sun, A Hahn, CC Liu. 2018. "Cyber-security of a power grid: State of the art." *Electrical Power and Energy Systems* 45-56.
- E. Karangelos, L. Wehenkel. 2022. "Cyber-physical risk modeling with imperfect cyber-attackers." *XXII Power Systems Computations Conference -- To Appear*. Porto. <https://arxiv.org/abs/2110.00301>.
- H. He, J. Yuan. 2016. "Cyber-physical attacks and defences in the smart grid: a survey." *IET Cyber-Physical Systems: Theory & Applications (IET)* 13:27. <https://doi.org/10.1049/iet-cps.2016.0019>.
- I. Zografopoulos, J. Ospina, X. Liu, C. Konstantinou. 2021. "Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies." *IEEE Access*.
- J. Zhang, Z. Chu, L. Sankar, O. Kosut. 2018. "Can attackers with limited information exploit historical data to mount successful false data injection attacks on power systems." *IEEE Transactions on Power Systems* 4775-4786.
- J.E. Sullivan, D. Kamensky. 2017. "How cyber-attacks in Ukraine show the vulnerability of the U.S. power grid,." *The Electricity Journal* 30 (3): 30 - 35.
- L. Duchense, E. Karangelos, L. Wehenkel. 2020. "Recent Developments in Machine Learning for Energy Systems Reliability Management." *Proceedings of the IEEE* 108: 1656-1676. <https://hdl.handle.net/2268/246570>.

- M. A. Rahman, H. Mohsenian-Rad. 2012. "False data injection attacks with incomplete information against smart power grids." IEEE Global Communications Conference (GLOBECOM). 3153-3158.
- NERC. 2019. Lessons Learned -- Risks Posed by Firewall Firmware Utilities. North American Electric Reliability Corporation. [https://www.nerc.com/pa/rrm/ea/Lessons%20Learned%20Document%20Library/20190901\\_Risks\\_Posed\\_by\\_Firewall\\_Firmware\\_Vulnerabilities.pdf](https://www.nerc.com/pa/rrm/ea/Lessons%20Learned%20Document%20Library/20190901_Risks_Posed_by_Firewall_Firmware_Vulnerabilities.pdf).
- Potvin, Marc. 2019. "The AURORA vulnerability: The sword of Damocles over the heads of rotating machines." 2019 CIGRE Canada Conference. Montreal, Quebec: CIGRE. <https://cigreconference.ca/papers/2019/CIGRE-244.pdf>.
- Slowik, Joe. 2019. Crashoverride: Reassessing the 2016 ukraine electric power event as a protection-focused attack. Dragos Inc. <https://pylos.co/wp-content/uploads/2021/02/crashoverride.pdf>.
- Smart Grid Coordination Group. 2012. Smart Grid Reference Architecture. CEN-CENELEC-ETSI [https://ec.europa.eu/energy/sites/ener/files/documents/xpert\\_group1\\_reference\\_architecture.pdf](https://ec.europa.eu/energy/sites/ener/files/documents/xpert_group1_reference_architecture.pdf).
- The Smart Grid Cybersecurity Committee. 2014. NISTIR 7628 Revision 1. US Department of Commerce. <http://dx.doi.org/10.6028/NIST.IR.7628r1>.