Challenges and Attributes of Future Energy Cyber-Physical Systems

Gabriela Hug, Soummya Kar, Philip Koopman, Bruno Sinopoli
ECE Department, Carnegie Mellon University, Pittsburgh, PA, United States
{ghug, soummyak, koopman, brunos}@cmu.edu

***Abstract*—The deployment of more and more sensing, information and communication technology has turned the electric power system into a prime example for cyber-physical systems. The key desirable attributes of such energy cyber-physical systems are efficiency, flexibility and resiliency. In order to achieve these attributes, the control structure of the future electric power systems needs to be designed keeping in mind the future characteristics of the grid infrastructure and the mutual interactions of the physical and the cyber system with the objective to ensure effective usage of the available equipment and sensed data.**

Electric energy systems are the largest and probably most complex man-made systems. Yet we take it for granted that we have reliable electric energy supply at all times. Whenever a major outage occurs, it results in large economical losses and causes significant disruptions to our daily lives. With the intended transition to more variable and distributed energy resources, integration of demand response capabilities and distributed storage resources, the number of controllable points and thereby the complexity of operating the system significantly increases. In order to ensure reliable and safe operation of the grid, more communication, sensing and information technology to collect high resolution data with the purpose of enabling intelligent decision making is deployed turning the power grid into a prime example for cyber-physical systems.

The most important attributes of the future cyber-enabled power system are: efficiency, flexibility and resiliency. In the following, we discuss each of these attributes in more detail.

Efficiency: Given that electric power is such a fundamental need of modern society, the grid is generally operated with significant margins to prepare for unexpected system events. It is basically operated in the sense of “better safe than sorry”. Here, we do not just refer to preventive actions which are taken to cover low probability events but also to the choice of conservative static operational settings and limits such as of transmission lines, transformers, breakers, etc. This leads to inefficient usage of grid equipment most of the time. The availability of real-time data and capability for fast reactive decisions allow for more granular and dynamic settings of operational limits as well as for corrective actions by fast-reacting devices, e.g. based on power electronics.

Flexibility: Renewable resources such as wind and solar power are not just variable and intermittent but also hard to predict which increases overall uncertainty in the system and makes efficient scheduling of balancing resources difficult. Consequently, the grid infrastructure as well as demand and supply need to become more flexible. However, it is not sufficient to simply add more flexibility to the system. The key questions are going to be how much flexibility is needed without sacrificing efficiency and how to make optimal use of the available flexibility. For the realization of the latter, the cyber system will be a key enabler.

Resiliency: The overlay of the physical system with an extensive cyber system promises to allow for a more efficient and proactive operation of the power grid. However, it also increases the number of possible points of failure and vulnerabilities in the system. This includes naturally occurring disturbances and delays in the communication system but also malicious interception of data sent in the cyber system. Hence, it is of utmost importance to carefully design a control structure which ensures fail safe mechanisms, detection and localization of failures in the cyber system. Key measures include (1) adding controlled redundancy in the sensing and actuation to ensure robust dynamic observability and controllability; (2) the design of *proactive* control mechanisms, i.e., adaptive control mechanisms that embed continuous detection and localization of malicious activity, to mitigate the effect of cyber threats on system performance; and (3) formal verification and validation of control algorithms and embedded control software under actual fault injections.

We believe that the current control infrastructure and current use of information technology is not suitable to achieve these attributes. There is a clear disconnect between the existing centralized structure and the distributed physical structure of the future electric power system. Distributed approaches are necessary to be able to coordinate and handle thousands of controllable elements in the system and render the system efficient, flexible and resilient. However, the control structure should not be chosen to be distributed just for the sake of being distributed. The design of the distributed control structure and choice of the right level of distributedness is very important and may result in a hybrid approach in which advantages of distributed and centralized structures are effectively integrated.

Currently, the cyber system is considered to be an add-on to the physical system which is useful to operate the power grid by enabling the sending and receiving of data. However, with increased dependency on the cyber system, the cyber and the physical system should be viewed as equivalent systems affecting each other. This includes the modeling, simulation and operation of the two system but also any approaches which address and enable the attributes described in this text. With an inefficient usage of the sensing and information technology, potential efficiency improvements in the physical system get lost. By this we refer to delays and outages in the communication system but also the fact that the availability of high resolution data does not mean availability of information, i.e. methods to extract useful information from available data are indispensable.

The above mentioned three attributes are to a certain degree antagonistic, i.e. optimizing for one may lead to compromising one or both of the others. E.g. ensuring resiliency may require to sacrifice some of the otherwise achievable efficiency and the same also holds for having enough flexibility available. Concluding, it is crucial to find the right balance between efficiency, flexibility and resiliency. The objective should be to ensure that the system is as efficient as possible while ensuring sufficient flexibility and resiliency.