A position Paper Submitted to the NSF 2013 Energy–CPS Workshop

Architectures, Cyber–Physical Co–Modeling and Vulnerability Monitoring for Power Distribution Systems

Dr. Fernando Mancilla–David⋆ and Dr. P. Papantoni–Kazakos †

In this position paper, we target the development of effective **cyber–physical architectures** and their subsequent **co–modeling** for power distribution systems. The focal point is the development of models and theories which will dictate clusterization of the distribution system, to construct cyber–physical–systems (CPSs) comprised of optimal–sized clusters that follow the microgrid concept, but also observe cyber demands and constraints. In particular, we seek the development of a unified cyber–physical optimization tool for the clusterization of current distribution networks, including the architectural organization of the evolving clusters. The steps of such development are: (*i*) a systematic mathematical modeling of distribution assets including physical and cyber components; (*ii*) design of optimization algorithms for clusterized system architectures which observe both physical and cyber demands and constraints, including performance monitoring and **vulnerability monitoring** automated techniques.

In power distribution systems, main design objectives include efficient operation, high penetration of renewables and distributed generation (DG), active load control, improved reliability, and self–healing. These objectives could be achieved through the fast control of hundreds of individual renewable and DG units. However, this would require real time information on each unit and key loads. The control complexity and reliability of such a system may be greatly reduced when the coupled microgrids are used. Then, the distribution system is broken down into smaller microgrids or clusters, with distributed optimal controls coordinating multi–clusters.

The intelligent scheduling of renewables, DG, and loads within a cluster may also improve the power quality to the consumer through ancillary services, such as voltage and frequency regulation, power factor correction and islanding during disturbances on the main network. Scheduling and power quality enhancement can be achieved through smart dispatch and control of the power converter that serves as an interface between renewables, DG and (possibly) loads and the distribution feeder. Existing power converters used as interfaces for renewables and DG are mostly dedicated to inject active power into the distribution feeder, with little or no capability to provide ancillary services. Therefore, clusterized operation may allow to fully utilize the control capability of power converters and hence improve overall system performance within the cluster.

Current distribution systems are mostly meshed systems, though operated radially. Feeders are made up of indivisible sets of loads and segments of distribution wire that connect to other sets through so–called "tie switches," forming a number of radial feeders. As a first approach, clusters may be formed by properly defining the status of the various tie switches, with the possibility of dynamic reconfiguration through switches operations. Radial operations may or may not be preserved, with the understanding that the latter would require an update of the protection system. A second, and more interesting approach calls for the use of back–to–back (BTB) power converters

⋆ Assistant Professor, Department of Electrical Engineering, University of Colorado Denver, Tel: 303–555–6674; `Fernando.Mancilla-David@ucdenver.edu`

† Professor, Department of Electrical Engineering, University of Colorado Denver, Tel: 303–556–3915; `Titsa.Papantoni@ucdenver.edu`

for the realization of the clusters' interconnection. Under this scenario, the clusters, while capable of operating as energy islands, will be able to also exchange power with each other. Furthermore, interconnecting clusters through BTB converters will allow for a controlled power exchange and asynchronous operation between the clusters. The former will lead to greatly improving reliability and economic operation while the latter will make the updating of the protection system unnecessary. We speculate that the utilization of BTB converters for cluster interconnection will be a significant factor in the success of the clusterization new paradigm in distribution networks. We may point out that BTB converters have been successfully utilized as asynchronous ties at a wide range of throughput power, from a few kilowatts in the motor drive industry up to several hundred megawatts as HVDC interties. For clusters' interconnection, throughput power levels will be in the order of a few tens of megawatts; therefore, the technology should be readily available.

Clusterization becomes a necessity when cyber issues are considered; that is, the flow and processing of data generated in the distribution network: cluster sizes are then dictated by the nature of the users and the data rates generated, in conjunction with bandwidth constraints and data accuracy/latency requirements, where, in the smart grid environment, various natures of users are represented, for example, by homes, industrial plants, electric cars and sensors. The data operations in each cluster are partially autonomous and implemented by existing technologies, while linked cluster heads (CHs) or aggregation and forwarding nodes (AFNs) comprise a backbone network which assures cluster connectivity. The topological design of the cyber clustered network should be dictated by its data processing and transmission operations and requirements, in conjunction with its physical layer characteristics (i.e. noise and data models, noise levels, fading factors, etc.), for the satisfaction of pertinent data processing performance versus communication cost versus mobility (electric vehicles)/survivability tradeoffs. In particular, such are the issues that should determine the formation (or not) of clusters and their sizes, as well as the possible connection of CHs and data fusion centers via feedback channels. For a variety of data processing objectives, the formation of network clusters presents a tradeoff. Cluster formation is beneficial when: (*i*) Each cluster covers a geographical area with relatively reduced noise and fading effects; (*ii*) The number of sources/users in the cluster is simultaneously sufficiently large to benefit from the communication cost versus latency tradeoff (reducing bandwidth waste, while latency in data transmission is maintained at tolerable levels); and (*iii*) The rate of data generation in the system is also sufficiently low to induce reduced probability of extraneous interference/collision effects, especially if wireless transmissions are deployed.

In view of the above discussions, clusterization of the distribution network is dictated by both power distribution and cyber considerations, where the location and size of the clusters are determined by both power and cyber limitations and requirements. It is eminent that specific power distribution and cyber performance metrics for clustering be identified and precisely defined, before a specific approach to clusterization be proposed. Such an approach will not only dictate the initial design of the clustered network, but will also subsequently dictate cluster reconfiguration and system self–healing techniques; when performance requirements/constraints are violated due to considerable changes in power or data flows, such changes may be communicated to the clusters via the cyber network initiating pertinent reconfiguration techniques in the cluster network. This approach naturally necessitates the continuous monitoring of the pertinent performance metrics, including those associated with system vulnerabilities; thus, inducing vulnerability monitoring.

The nature of the posed cyber–physical problem does not allow for a closed–form formulation. Instead, a mathematical programming problem may be formulated in the physical domain; subject to both physical and cyber constraints, while the satisfaction of the cyber constraints may be attained via continuous performance monitoring and dynamically adjusted cyber operations.

As may be concluded from the above discussions, performance monitoring is the indispensable component in the cyber–physical system management. Effective performance monitoring may be accomplished if the important system performance metrics are first identified; together with their statistical characterizations under various scenarios, and if statistically reliable algorithms are subsequently deployed for the continuous monitoring of these metrics and the subsequent recognition of alarming changes. A performance monitoring system (PMS) will be comprised of several sequential algorithms, some of which will be monitoring vulnerability metrics. We point out that current technology permits the implementation of a PMS system.

The PMS may be deployed at the cluster heads or base stations. It will dynamically compute the pertinent performance metrics and will continuously compare the found numbers against those predicted by the performance analysis of the deployed cyber–physical operations. As a result of this comparison, the PMS will estimate characteristics of the user populations (power and data traffic intensities, for example). Using these estimates, in conjunction with pre–computed performance characteristics of the deployed operations, the PMS will then dictate appropriate changes in system operations and possibly architectures. The effective design of the PMS implies thorough quantitative studies of the deployed cyber–physical operations. The results of such studies may be maintained in memory to be used for operations adaptations and possible architectural reconfigurations.

⋆ ⋆ ⋆ ⋆ ⋆

Fernando Mancilla–David received the B.S. from Federico Santa María Technical University, Valparaíso, Chile in 1999, and the M.S. and Ph.D. degrees from the University of Wisconsin–Madison, Madison, WI; respectively in 2002 and 2007, all in Electrical Engineering. He has been an assistant professor in Electrical Engineering, at the University of Colorado Denver, since 2007. He has been a visiting scientist at various European academic institutions. He has coauthored more than 40 refereed technical papers, mostly in the area of utility (transmission and distribution) applications of power electronics. He is a member of IEEE.

P. Papantoni–Kazakos received the Diploma in Electrical, Mechanical and Industrial Engineering from the National Technical University of Athens, Greece, in 1968; the M.S, degree from Princeton University, Princeton, NJ, in 1970; and the Ph.D. from the University of Southern California, Los Angeles, CA, in 1973, both in Electrical Engineering with specialization in Statistical Communications and with minor in Mathematics. She has been in the academia since 1973, where she is currently professor of Electrical Engineering at the University of Colorado, Denver. Her research interests include Statistical Decision Theory, Distributed Processing and Neural Network Structures, Statistical Communications, Information Theory, Robust Statistical and Encoding Methods, Stochastic Processes, Computer Communication Networks and organizational networks. She is coauthor of two books and more than 260 refereed technical papers. She is a Life Fellow of IEEE, for "Contributions to Communication Networks and to Detection and Estimation Theory".