Resilient Control Architectures & Systems (ReCAS)
A multi-agent approach to a Smart Grid

Craig Rieger, Idaho National Laboratory

Hurricane Sandy bluntly reminded us how much we take for granted the complex systems that provide energy, transportation, water, medical care, emergency response and security at levels considered luxurious just a generation ago. A presidential policy directive issued in February, "Critical Infrastructure Security and Resilience," [[link to: http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil]] recognized the need to advance R&D to strengthen system models and design, facilitate secure information exchange and enable more effective decisions and investment.

Control systems play an ever-increasing role in critical infrastructure performance and protection. But today's designs fall far short of being the widely imagined highly autonomous and flexible systems that are supposed to be at the heart of efficient, effective and resilient critical infrastructure. In truth, most modern control systems are little more than digital versions of the analog architectures they replaced. While these networked platforms have provided a reliable means to establish central monitoring and have eased integration of feedback/supervisory controls, these systems have only a limited ability to recognize infrastructure degradation wherever it may occur and optimize a corporate response is limited. And so proper operation of any critical infrastructure facility continues to be heavily dependent on human interaction.

Meanwhile, the ability to network distributed components is producing additional interdependencies, resulting in even greater system rigidity or brittleness, which in turn increases the likelihood of cascading failures.

Yet the opportunity also exists to leverage the dramatic capability gains in networked digital devices and sensors to expand functionality, such as real-time self-monitoring and condition analysis, to detect and respond to anomalies and incipient failures. Operators and dispatchers can be liberated from the impossible task of interpreting mountains of "big data" to become informed, proactive system managers. At the same time, next-generation control systems could dramatically improve global production efficiencies, all the while monitoring for potentially disruptive natural or hostile events.

A multi-agent philosophy has been proposed as a notional architecture to decompose these control system dynamics and interdependencies in a smarter grid. Many perspectives exist, but the ultimate design objective generally is to achieve resilience to threats while providing a platform for greater autonomy. To consider how a multi-agent system might apply to a power grid, let us reflect on how this system might look at the execution layer of a traditional 3-layer multi-agent hierarchy defined as follows:

- *Upper Layer—Management*. This event-based layer provides the overall philosophical goals and priorities for operation. The sources for this design range from management and regulators to the physical constraints of the system.
- M*iddle layer—Coordination*. This event-based layer provides potential realignment of resources that best enables meeting the dictated philosophy. This layer drives the execution layer.

- *Lowest Layer—Execution*. This time-based layer provides direct monitoring of sensors and control of field devices.

Within the execution layer, a level of autonomy is provided between peers to achieve a control response in parallel with the dynamics of the layer. For greater effectiveness, decomposition of the plant operations must be done in a way that maximizes the uniformity between peer operations to enable resource sharing. The promise is to allow a level of autonomy between peers to enable rapid adjustment of the plant to reflect shifts in operation and to counter threats and disturbances. This is important, as the response time increases when a response is dependent upon interaction with the management layer of the hierarchy.

Considering the operation of a generation plant, a decomposition principle is already implied by current control system designs. That is, execution layer elements are associated with unit operations or some optimally stabilizable entity. The unit operation, in this case, defines an area of local optimization. Within the operation, many physical variables may exist. In a plant made up of many unit operations, the process of determining the optimally stabilizable entities normally results in a minimization of the interactions between individual unit operations. That is, normally only a few physical variables will make up the interactions between unit operations. For example, the flow and thermodynamic characteristics of steam from the boiler to the turbine must remain within a specified range, as the downstream operation is designed to be stabilized for operation within that range.

The process of determining unit operations also might suggest an approach for the execution layer of a smart grid multi-agent dynamical system. As a transfer function would provide a conventional approach to controlling individual unit operations, extrapolating this concept would seem reasonable. That is, a transfer function should exist that describes the interaction and provides the dynamics of operation, including control and plant dynamics. Consensus control techniques that utilize a graph Laplacian can then be applied to ensure a physical certainty of overall system stability.

While this concept is directly applicable to a power generator, its application to distribution and transmission infrastructure and the integrated power system is more challenging. Clearly current power grid implementations depend upon varying generation to fulfill load requirements through bulk power transmission and distribution, which is not conducive to this idea. Nevertheless, with growing interest in establishing micrograds at military bases and university campuses, and in direct load controls such as demand response, some fundamental infrastructure elements are already being pursued to base execution agents.

Defining the execution agent as above provides the needed context to identify and apply recognition, selection and graceful degradation techniques. Cyber degradation, like physical degradation, must also be recognized in the context of the optimally stabilizable elements of an execution agent. While recognition techniques may differ, the selection and graceful degradation mechanism will be common. The ability of the execution layer agents to optimally achieve consensus, and ultimately the resilience of the distributed control system and its associated industrial plant, is dependent upon this recognition.

Briefly considering the management and coordination layers that “supervise” the execution layer, these layers of a multi-agent architecture provides a framework to codify human-centric beliefs, desires and intentions in operating the grid. Establishing performance and coordinating assets within a distributed control system design provides for a reduction in inefficiencies and inconsistent application of management policy. In addition, the benefits received from reducing the inefficiencies can be applied, in part, to dealing with anomalous, emergent behaviors. As a means of embedding human expert knowledge into an agent and producing optimal decisions, fuzzy logic provides recognized benefits. In similar light, a Bayesian design provides a means to characterize historic results, even with partial observability of states, into coordination agents.

Resilient control architecture and systems approaches, such as the multi-agent approach described, are needed to prevent and/or deliver appropriate response to reoccurring major events that impact critical infrastructures such as the power grid. Federal government R&D investment in next-generation control system architectures will be required to achieve a more autonomous, gracefully degrading smart grid. This investment will revolutionize current designs that to date have been left to evolve organically in the private sector, providing very reliable systems but lacking the threat resilience needed to address unforeseen natural and manmade events.