Resilient Control Systems
A Multi-Agent Dynamic Systems Perspective

2013 IEEE International Conference on Electro/Information Technology

Craig G. Rieger
Kevin L. Moore
Thomas L. Baldwin

May 2013
Resilient Control Systems
A Multi-Agent Dynamic Systems Perspective

Craig G. Rieger
Senior Member, IEEE
Idaho National Laboratory
Idaho Falls, Idaho, USA

Kevin L. Moore
Senior Member, IEEE
Colorado School of Mines
Golden, Colorado, USA

Thomas L. Baldwin
Fellow, IEEE
Idaho National Laboratory
Idaho Falls, Idaho, USA

Abstract—“Resilience” describes how systems operate at an acceptable level of normalcy despite disturbances or threats. In this paper we first consider the interdependencies inherent in critical infrastructure systems and how resilience mitigates associated risks and then define “resilience” in distinction from conventional control engineering. We then introduce the concepts “agent” and “multi-agent systems” (MAS) to consider the distributed nature of critical infrastructure control systems and illustrate the application of computational intelligence to MAS event-based dynamics (management, coordination) and time-based dynamics (execution) to manage policy and coordinate assets. In addition, we consider the optimal stabilization of the MAS and suggest the extension of graph theory to MAS execution layers. The closing discussion provides an overview of how to achieve critical infrastructure resilience through advanced control engineering.

Keywords—Multi-agent systems, resilient control, distributed control, consensus, networked dynamic systems, graph theory.

I. INTRODUCTION

A. Critical Infrastructure Systems

Modern societies depend on the stable, efficient, and secure operation of critical infrastructure. While “infrastructure” may refer to such static assets as the roads and highways that connect our cities and the power lines that distribute electricity to our homes and businesses, we are concerned here with “infrastructure systems” by which we mean interconnected and interoperable assets. In other words, critical infrastructure systems comprise “...a set of interconnected components working together towards some common objective”.

For example, when we consider the electrical grid, we include the power lines that deliver electricity as well as generating plants, substations, voltage regulators, transformers, etc. Most critically, we expect and indeed depend on such systems of interconnected and interoperating components to deliver electricity of suitable quality at an affordable price without interruption even when things go wrong.

In conventional terms, control engineers achieve system stability, efficiency, and security by both static and dynamic means. On the one hand, control engineers achieve static coordination by ensuring that the physical interfaces between and the functions of system components are compatible. This is achieved through the initial selection and design of system components. On the other hand, control engineers achieve dynamic coordination with control strategies that enable systems to detect and respond to operating environment changes. Such changes include system component or interface failures or malicious threats from outside the system. The next section of this paper will describe how, outside of the improved physical design of system components, resilience is primarily achieved through dynamic coordination.

B. Resilient Control Systems

The following is adapted from [1], which provides the definition:

A resilient control system is one that maintains state awareness and an accepted level of operational normalcy in response to disturbances, including threats of an unexpected and malicious nature.

The “resilient control system” (RCS) is arguably a new control design paradigm that encompasses cyber-security, physical security, economic efficiency, dynamic stability, and process compliancy in large-scale, complex systems. From a conventional control engineering perspective one might say that an RCS is merely dependable computing coupled with fault tolerant control, however, we argue [2] that this perspective is too narrow. For example, while the fault tolerant control community has developed ideas of fault detection and identification and to some extent the ideas of reconfiguration, these are not readily linked to control response; nor does the control community have a way yet to systematically consider faults resulting from the cyber-environment associated with the system. RCS attempts to synergistically capture both the cyber and the physical aspects of system design and operation, thereby overcoming the limitations of the reliable computing and fault tolerant control perspective.

Indeed, there are two key limitations of conventional control engineering that support the need for resilience, and in turn, multi-agent design. First in practice, conventional control engineering primarily focuses on lumped parameter systems. By this we mean the system and its inputs and outputs are assumed to be “lumped” in space and thus modeled by ordinary differential or difference equations. As noted in [3] “…essentially everything done in the last 50 years of control engineering rests on a common presumption of centrality [that all the information available about the system, and the calculations based on this information, take place at a single location]…” Interestingly, this quote was made in 1978! In
the same article it is also noted that “... power networks ... urban traffic networks ... digital communication networks ... flexible manufacturing networks ... are often characterized by geographic separation so that issues of reliability of communication links have to be taken into account, providing impetus for a decentralized scheme.”

Second, although digital controls are now common and many control systems are implemented through commercially-available distributed control systems (DCS), which we will also refer to here as networked control systems (NCS), control engineering is only now beginning to develop theory that takes into account the fact that modern control systems are almost exclusively implemented over computer networks [4]-[7]. There are two aspects to this limitation. One is that conventional control engineering does not address the fact that many decisions made in a DCS are “logical” decisions (e.g., “if the temperature is greater than a threshold, then turn off the heater and open the valve”). The developing theory of hybrid control attempts to deal with the discrete event-based nature of large-scale DCS systems together with the underlying lumped aspect of the subsystems that make up the overall system. Secondly, conventional control engineering does not systematically account for how DCS systems network communication protocols affect overall system performance.

C. Paper Outline

In the foregoing, we discussed the need for a new control engineering paradigm that we term “resilient control systems” as a means of moving beyond conventional control engineering. We suggest that conventional control engineering theory is ill suited to deal with both the cyber and physical control challenges emerging in the early twenty-first century because these theories were developed in response to control systems characterized by spatially-lumped models and discrete events. In what follows, we take up the notion of “multi-agent systems” (MAS), which we suggest offers a notional framework for controlling not only physical systems but also cyber systems and the hybrid interplay between the two. Section II begins with a discussion of the basis for selecting MAS design as a way to characterize distributed control and details some of the attributes that require consideration. Section III provides a broad overview of how the event-based decisions that form the target of control system performance and the time-based execution elements are defined, i.e., decomposed from the system attributes into interacting agents. Section IV describes the layers of a MAS and also proposes an overall theory to codify the layers, including the execution (and plant) layers based upon dynamic network theory. Section V provides a framework for design of a hierarchical multi-agent dynamic system (HMADS) using a notional example from the power system as a basis. In conclusion, this paper provides a research strategy for implementing an HMADS, extending some existing methodologies with a framework to utilize these methodologies within the paradigm of distributed control system architecture.

II. MULTI-AGENT SYSTEMS (MAS)

A. Why Multi-agent Design?

1) What is an agent?

The suggestion of agents was developed as a mechanism to describe objects, “informing, requesting, offering, accepting, rejecting, competing with and assisting one another” [8], [9]. Early development of agent identities were directed toward artificial intelligence in computer science applications [10], as compared to the dynamics of control. The definition of an agent is varied, depending upon its application [11],[10] For the purposes of this paper, the characteristics of an intelligent agent are the most applicable. In general, an intelligent agent can be described as a semi-autonomous entity that evaluates the state of its environment and applies control actions towards achieving goals within this environment, such as is depicted in Fig. 1. By semi-autonomous, the implication is that the agent has a predefined sphere of influence that establishes the boundaries of its autonomy. Considering the definition for a resilient control system, a further refinement can be made. It follows that a “resilient” intelligent agent is one which maintains a state awareness of its environment and responds to disturbances in order to maintain operational normalcy within this environment.

2) How has agent design been standardized?

The Foundation for Intelligent Physical Agents (FIPA) was developed to frame standards for agent communications. Based on its semantics, works have been written to extend these semantics to a control system format [12], [13]. While future multi-agent implementations may find basis in the use of these semantics, and in fact have in current tools like JADE [14]-[16], the larger issue to be addressed and understood is the mechanisms by which improved performance, and ultimately resilience can be achieved. Evidence in this regard is necessary, and to be affective as a design standard should be broadly applicable to a variety of applications and scales.

In an effort to develop a more modular framework that is more reflective of an agent based design, IEC-61499 has been developed. This standard defines the building blocks of a distributed control system based upon a function block implementation. However, while it provides a mechanism for event-based control, its application is rather an extension of current methodologies for implementing low-level control algorithms into control system software [17], [18].
3) How has multi-agent design been applied?

While a number of different alternatives have been proposed for distributed control system design, few provide the level of integration necessary to support claims of superior performance over traditional designs. The idea of graceful degradation has been with us for several years, with many contributing theories, however it is often only verified on rather small scale demonstrations.

Efforts targeted toward multi-agent design, including control system applications have included [19]:

- Development of specifications for fundamental agent structure and communications
- Control stability arguments of agent structures
- Consensus of agent resource use

Other related developments have focused on mechanisms to understand the effects of latencies or complex interactions on advanced control design [20].

B. MAS Issues for Distributed Control

There are a number of issues associated with the use of MAS in distributed control applications. Here we highlight three significant ones.

1) Subsystem versus Global system

Traditional mechanisms of ensuring global stability were to ensure local performance of individual subsystems, and assume as a collective that local stability equates to global stability. While this mechanism remains the most practical, its flaw lies in the fact that an understanding of global performance as a feedback measure is not achieved. So while first principles modeling of large systems may be untenable from a practical standpoint, due to issues of computational power, sparesness of systems, etc., mechanisms are needed to determine what the global optima is. In addition, global efficiency as well as stability are important to next generation designs.

2) Stability of Hierarchy

Several researchers have developed proofs for stability of multi-agent, networked architectures [20]. However, these proofs and their associated assumptions fall short in providing a robust mechanism for defining the stability of complex networked control systems. Some specific details that must be addressed in the development of proper stability arguments need to consider or address the necessity of the algorithm used for the controller. As many types of algorithms can be used, and at its heart multi-agent designs are intended to be reconfigurable, options for changing the type of algorithm based upon application or environment should still provide stability when applied per a known design basis.

3) Metrics

In addition to developing an integrated approach to multi-agent design, a method of baselining performance is necessary. This is no easy matter, as resilience considers the complex interactions within control systems [21], which include malicious and human error. Therefore, metrics do not exist to confirm the aspects of resilience from a holistic context, and must be created for resilience research to have relevance.

C. Resilience Issues for Distributed Control

There are a number of issues to consider when addressing the notion of resilience in a control system. In this subsection we discuss four of these: latency, physical degradation, cyber compromise, and human performance.

1) Latency

Consensus and feedback loop stability can be affected by latencies in the communication and computational processes of the control system architecture. Research into the effects and constraints on latencies has been performed to determine stability [20]. Several different approaches have been taken, including evaluating the impact on an individual control algorithm and determining maximum acceptable latency. Other methodologies have characterized latency as part of the overall dynamics of a multi-agent hierarchy, representing communications links as transfer functions between individual agents that are stabilized by a given control algorithm [22].

2) Physical Degradation

Dependence upon sensor data for judgment dictates that a method of graceful degradation is needed to monitor health and change sensor combinations used to achieve observability and controllability. In addition, the characterization of a physical attribute may include modeling coupled with a sensor, or strictly synthetic data from a mathematical observer. The sensory framework, therefore, must provide methods for interpreting information quality, in addition to sensor and control device redundancy and diversity to allow for reconfiguration based upon failure [23], [24]. From a control perspective, similar considerations are necessary to enable maintaining critical control when failures are detected. This may include access to alternative paths and associated controls, but not necessarily switching of components (parallel paths may be online at all times).

3) Cyber Compromise

Traditional mechanisms of detecting failure based upon first principles modeling or intelligent techniques do not provide a firm conclusion of evidence of a cyber security attack. While the affects of cyber attack may be to create latency, the impacts may be more direct and include data modification. In addition, the impacts may be diverse in what elements of the distributed control system are affected. Therefore, diagnostics that include diverse measures of cyber health are needed, including methods to observe affects on the data for current [25] and multi-agent designs [26]. In addition, a consistent approach to recognition and response of cyber and physical degradation [23], [24] is necessary to ensure resilience in a multi-agent design. While the referenced framework is inherent to the time-based dynamics of multi-agent design, an event-based approach is also necessary.

4) Human Performance

Human performance can be a benefit and a detriment to the stability of a multi-agent system, but regardless is a necessary
component [27]. The interaction of the human at various aspects of the design process can affect the resilience of the distributed control system. The interaction can range from the direct selection of operating states to the overall direction of system performance as dictated by profit motivations, environmental concerns and related issues. Instead of considering the human as a risk to be compensated for, however, a tailoring of automation to the needs level of the user is required [28] to provide increased system resilience. From a system performance perspective, a mechanism of decomposing the often conflicting requirements that are the basis for operation must also be normalized.

### III. NOTIONAL MULTI-AGENT FRAMEWORK

In this section is a brief description of the MAS hierarchical layers and dynamic interactions is provided, hereafter designated as Hierarchical Multi-agent Dynamic System (HMADS) [29]. The proposed framework is a collective method to pair the human-driven operational philosophy for an industrial plant with the dynamics of the control itself.

#### A. Decomposing Operational Philosophy into Multi-agents

While multiple layers can be imagined, for the purposes of illustration three are suitable to identify distinct and separate functionality [30], defined as follows and illustrated in Fig. 2:

- **Upper Layer—Management**
  
  This layer provides the overall philosophical goals and priorities for operation. The sources for this design range from management, regulators, physical constraints of the system, etc.

- **Coordination layer—Coordination**
  
  Coordination provides potential realignment of resources that best enables meeting the dictated philosophy. This layer drives the execution layer.

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

### B. Decomposition of Operational Philosophy into Management and Coordination Layer Multi-agents

There are several factors that influence the philosophies that govern how performance goals are set, and these factors require consideration when establishing the policy of the management layer. However, understanding what these factors are and developing a method to decompose them down to constraints of operation are important. In some cases, the constraints are cut and dried. In others, however, an interpretation must be made by those in authority. Below is a list of some factors that should be considered with control system decomposition:

- Regulatory Requirements: Considering primarily governmental agencies that regulate the operation or its products in some fashion is a key responsibility at this layer.

- Desired Performance: Whether a production rate or an efficiency objective, this aspect comes from a desire to maximize profit for the organization using the control system.

- Physics-based Limitations: The physics of the design affect the limits of the operation. While this might seem obvious, one must collectively include this when considering the tradeoffs of performance.

Establishment of a coordination layer requires a mechanism to connect management policy to execution dynamics, establishing a resilience buffer to maintain operational normalcy. In its simplest form, this connection can be considered setpoints, or even a mathematical relationship that allows flexibility in operation but also constraints execution to a given set of dynamics. Unlike traditional concepts of setpoints established to prevent violation of operational limits, however, here the discussion is the development of overall resilience buffers by the nature of the design to achieve optimal performance and prevent loss of critical operation. Below are some of the aspects that can be considered in the coordination layer decomposition:

- The dynamics of the system requires tracking of the optimum path or trajectory to achieve optimum stability, in addition to achieving local stability. Stated another way, the performance of the system remains within its constraints for operation. This implies a performance goal that considers path and endpoints.

- The ability to share, and ultimately negotiate resources is limited by the uniformity of the system. For example, an unmanned air vehicle squadron can provide a highly uniform implementation of a MAS, and therefore, a higher level of resource sharing is theoretically possible within the constraints of the design. The level of uniformity is defined, in this case, as the ability of an agent to provide a necessary functionality in the fulfillment of a need.

- Decisions for shifting of resources can occur at different layers of the MAS hierarchy, with control action taken at both the middle and lower layers. However, the goal of

---

**Fig. 2. HMADS Layers**
consensus is the same regardless of the level, which is to adjust resources to reach optimum performance. The difference lies in the sphere of influence. That is, the coordination layer has responsibility for multiple lower level agents, and as such, will better orchestrate shifts in operation to accommodate the performance goals of the management layer.

C. Execution Layer Interactions to Achieve Operational Philosophy Goals

The responsibility to operate based upon direction lies within the execution layer. Whereas in a traditional system these directions come from procedures, orders and judgment, a HMADS directly ties policy to execution. Considering the orchestration of individual agents, methods to achieve some overarching goal have been researched for the last two decades within the mobile robotics community [31]. Although industrial control systems control a different type of plant, effectively every robot forms a similar parallel in operation in that it includes the monitoring, analysis and control in one package with the plant. Some of these similarities that can be considered include:

- Decomposition to minimize, and as a result, simplify, agent interactions and complex dynamics
- Development of agent layers in a hierarchical structure
- Optimize inter-agent interactions with consensus theory to achieve a common objective
- Optimize inter-agent interactions with applicable control engineering, soft and hard computing, defined by most relevant to situation. The ultimate goal is to stabilize the shared manipulated and controlled variables.
- Whereas robots are effectively individual agents, an optimizable subset of an industrial plant can be characterized as an agent

D. Addressing Resilience in a Multi-agent Framework

Considering the resilience issues of the prior section in summary, a HMADS provides an adaptive framework to build technologies that are resilient. However, the HMADS design must possess certain attributes related to the issues of resilience as described above in Section II.C, as provided below:

1) Latency
Defining the execution agents by associating closely-related dynamic or optimally stabilizable elements of an industrial plant will effectively minimize the spatial context for control. As such, the communications distance, bandwidth and computational processing is effectively distributed and intuitively also minimized. Time-based consensus theory dynamics, which will be discussed in sections that follow, can provide a mathematical formulation to optimize the execution layer inter-agent interactions to achieve codified management goals [32].

2) Physical Degradation
Recognition of sensor and field device degradation is fundamental to accurately reacting to threats of stability to an industrial plant. Defining the execution agent as above provides the needed context to define and apply the recognition, selection and graceful degradation techniques. Due to the limits of space, a detailed discussion of these techniques is left to other works [23], [24].

3) Cyber Compromise
Similarly to physical degradation, cyber degradation must be recognized in the context of the optimally stabilizable elements of an execution agent. While the recognition techniques may vary from the physical attributes, 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. As with physical degradation, a detailed discussion of cyber techniques is left to other works [25], [33].

4) Human Performance
Within the management and coordination layers, a HMADS provides a framework to codify human-centric beliefs, desires and intentions (BDI) for operating the industrial plant. 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 within an industrial plant. As a means of embedding human expert knowledge into an agent and producing optimal decisions, fuzzy logic provides recognized benefits [34]. In similar light, a Bayesian design provides a means to characterize historic results, even with partial observability of states, into coordination agents [35]. These techniques as applied to a HMADS will be discussed in the sections that follow.

IV. METHODOLOGIES TO DECOMPOSE OPERATIONAL PHILOSOPHY

Decomposition of the guiding philosophy and performance by which a control system is operated can be considered qualitatively with relative ease. However, the assurance of reaching an optimal decomposition is challenge, as a portion of the reasoning reflects human decisions based upon varying information. Therefore, in what follows a qualitative approach is first presented and then a quantitative approach is given with restricting, but practical, assumptions to limit the variability of the decision.

A. Qualitative Aspects
In a 3-tier HMADS, the ultimate decisions for “global” performance occur at the top management layer with the middle coordination layer providing the interpretation and adjustment of control system settings. “Local” decisions are necessary to shift resources at the lowest or execution layer, primarily for inter-agent reconfiguration to account for component failures of the control system itself or the plant.

A level of autonomy is provided between peers to achieve a control response in parallel with the dynamics of the layer. To be effective, decomposition of the plant should be done in a
way to maximize the uniformity between peers. With an HMADS, however, the promise is to allow a level of autonomy between peers to enable rapid adjustment of the HMADS and plant. This is important, as the response time increases when a response is dependent upon interaction with the management layer of the hierarchy.

Considering the execution layer of a 3-tier HMADS, a decomposition principle is already implied by current control system designs. That is, execution (supervisory and device control) layer elements are associated with unit operations, substations, or some optimally stabilizable entity. This can be seen from looking at power generation plants, where a collection of separate unit operations make up an integral plant. 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 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 suggests an HMADS approach, at least at the execution layer. 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 then provides the dynamics of operation. From a hierarchical context, if a similar concept can be extrapolated to the middle and management layers, existing control engineering can be extended to stabilizing an HMADS. However, while the execution layer interactions are control system centric, i.e., directly associated with supervisory and device control, the coordination and management layers are not.

The management layer accomplishes a direct de-confliction in the constraints imposed on the control system, specifically desired performance, environmental restrictions and physics-based limitations. Computational intelligence techniques, such as fuzzy logic, provide a mechanism for this de-confliction, as it allows for a behavioral connection between human desires and actual plant performance.

In contrast, the coordination layer provides an element of discernment between past decisions based upon future targets of performance from the management layer. This discernment is only important in ensuring the real intent of the decision, but also in determining what the best decision might be to fulfill the desires of those governing the high level organizational objectives of the system. Past knowledge of decisions also provides basis for future and contrasting bad or malicious compromise. Confirmation of past experience based upon decisions provides a layer of protection from human mistakes and malicious interactions.

The next subsection splits between discussions of the layers that establish a management and coordination basis for the hierarchy, which have as their core a substantial human influence on the policy and strategy, and that of the execution (and plant) layer, which are based on typical control system dynamic interactions.

B. Quantitative Approach: Management and Coordination Layers

At the management layer of a HMADS, computational intelligence techniques such as fuzzy logic lend themselves to incorporation of human knowledge to a control design [34], [36], [37], while still allowing a “defuzzification” process to maintain the dynamical aspects. The information from the coordination layer is used as feedback to determine high level decisions based upon state awareness. In turn, the management layer establishes policy for the coordination layer, which will in turn use this as a basis to establish targets for operation in the execution layer. Considering a notional fuzzy logic implementation of such an approach to a notional power system, such as that illustrated in Fig. 3, the following framework can be envisioned:

- **Linguistic variables**: Unique identifier of policy decisions needed to establish the overall governing performance goals of the plant.
- **Membership functions**: The number equating to the decision alternatives and the shape based upon the confidence in each.
- **Rule base**: Performance goals matched with regulatory requirements and physical limitations of the design.
- **Output**: Policy for operation, using a defuzzification mechanism that suggests the appropriate amount of influence on the plant operation.

To optimize the settings for the referenced fuzzy framework, a multi-criteria, interdisciplinary method is needed to achieve a commonly accepted or more resilient decision. Several methods have been developed that use fuzzy logic as a technique for aggregating expert opinions [38]. Expert opinions and management team BDI for operation are expected inputs to this layer, which is similar to a dispatcher interacting with a supervisory control and data acquisition system (SCADA) to direct power through a transmission or distribution system. In the case, however, the management authority establishes the organizational goals for the operation of the control system.

Considering the example of Fig. 3 and a weights calculation [38], the management authority establishes the basis for making economic shifts. The weights \((w)\) for the multi-criteria are given as follows [39]:

\[
q_i = Q\left(\frac{i}{n}\right) - Q\left(\frac{i-1}{n}\right), i = 1, \ldots, n
\]  

\((Q(r))\) is a regular increasing monotone (RIM) quantifier that
Fig. 3. Notional fuzzy management layer decision for a power system

establishes the relationship weighting. Given that \( Q(r) \) is a quadratic function \( r^2 \) which provides a nonlinear preference to shared decision, such as shown in Fig. 4, the resulting weights from (1) are as follows:

\[ w_i = \frac{i^2}{n^2} - \frac{(i - 1)^2}{n^2} \quad (2) \]

\[ w_i = -\frac{2i + 2}{n^2} \quad (3) \]

The implication of this method of aggregating, therefore, is that the more individuals satisfied ultimately determine the decision selected [39]. Given Fig. 4 and the team \( n \) with management authority that codifies the economics agent, each individual \( i \) will make a judgment that provides the final membership functions and rules established for the rule base in Fig. 3.

The role of the managerial layer is to set a policy that reflects the performance goals for the HMADS. However, variability in human judgment and tradeoffs between different areas of performance can affect how the goal is established. History with the operation and the benefit of feedback can provide the expertise with an operation to ensure desires meet with reality, and a semblance of optimality is achieved. In addition, consideration of intent should include the potential for malicious actors obfuscating lines of communication. To codify this historic understanding of the HMADS plant, methods are necessary that integrate both the human and control system interactions. Bayesian reasoning is one method by which evidence of human tendencies can characterize past behavior [40], providing a basis for a level of resilience in addressing the coordination of field devices that is required to effect policy. Where more than one execution agent is available to fulfill the policy, the system provides the ability to respond in spite of failures and increased resilience.

Fig. 4. Decision Weighting on Expert Opinions
The decision to react can be a judgment of the Bayesian Belief Network (BBN), such as in Fig. 5, established for the implementation in the coordination layer. This interaction would be specific to larger impact issues, and complements data analysis that occurs at the execution layer itself that reacts to loss of sensory capacity. Summarizing, the coordination layer will need to take the high level operational philosophy from the various contributors, and normalize them into a “tag-based” or similar unique identifier to connect the corresponding direction given to the field devices in the execution layer.

Bayes’ Formula and the manipulated probabilities for the BBN can be more simply expressed in terms of a hypothesis (H) and data (D):

\[ P(H/D) \propto P(D/H)P(H), \]

where:
- \( P(H) \) is the prior probability of \( H \); the probability that the hypothesis is correct before comparing to the data.
- \( P(D|H) \) is the conditional probability; likelihood of seeing the data \( D \) given that the hypothesis \( H \) is true.
- \( P(H|D) \) is the posterior probability; the probability that the hypothesis is true.

For illustration of using Bayes formula, the coordination of a decision on affected generation plants can be considered. Per Fig. 5, shifts in generation sources consider the management layer policy changes, such as those indicated in Fig. 3. Given a prior probability from the defuzzification of the management layer, a relationship to take the place of what is performed verbally between humans currently. The closer the prior probability \( P(H) \) from the management layer is to “1,” the greater the focus is on generation according to Fig. 3. Assuming the conditional term in Bayes’ formula is already a normalized probability and is based upon data for the operational status and capacity, an indication on the availability and timing for modifying the operation of each generator \( (k) \) can be determined:

Select: \( P_k > P_{k-1} \) Given: \( \frac{P(D/H)}{P(H)} = \frac{P(D/H)P(H)}{P(H)} \).

Based upon the posterior probability, the most likely generator(s) for selection will be provided. The cost of producing power \( (p) \) for each generator \( (CF) \) and individual plants \( (k) \) is commonly associated with a standard quadratic form, where \( p \) is power output and \( a \) are constants [41]:

\[ CF_k(p) = a_0k + a_1kp + a_2kp^2. \]

A determination of the final generator mix for the “Negotiate shift” agent in Fig. 5 then becomes a straightforward cost optimization problem. However, shifts in generation will also consider efficiency (including security) and stability agents in order to allow a shift. A secondary Bayesian evaluation agent is needed for the “Generation alignment” and “Distribution alignment” agents. The resulting formulation will consider the

![Fig. 5. Notional BBN policy to field device coordination system for a power system](image-url)
priority to achieve the desired resilience. In the case of the power system this is stability first, then economics, and finally efficiency. In addition, the state estimation (conditional probability) is now based upon data from the execution layer agents that characterizes estimations in the ability of the generator to support shifts in demand [42].

Considering finally the execution layer, implementation of supervisory control (Fig. 6) is necessary to ensure the integration of the global policy with the specific contributions of each execution agent. Given an economic shift is decided by the coordination layer, the supervisory aspect of each generator or distribution asset would define the set points and alignment, respectively, to achieve the desired goals. Within the device layer, the types of multivariable control that can be brought are numerous, including $H_2$ and $H_{\infty}$, model predictive control, etc [43]. The benefit and practicality of any supervisory methodology will be dependent upon the plant application. However, perhaps the more important question to address is how the execution layer and its various sub-layer agent interactions can be stabilized. This topic is the focus of the next subsection.

C. Quantitative Approach: Execution (and Plant) Layers

Large-scale industrial or infrastructure systems are fundamentally dynamic systems. This is why we say that resilient control is more than a problem of computer reliability. It is the intersection of the problem of computer reliability with the stability and robustness aspects of the underlying dynamics of the system-to-be-controlled that complicates matters. Of course it is likewise true that the problem of resilient control is more than a dynamics problem. However, we contend that approaches that do not carefully couple the dynamics of the plant to the attendant cyber aspects of the system will not be resilient. What is needed is an approach to do this coupling. In this subsection we suggest a research direction in this regard that is based on graph-theoretic approaches to dynamic systems.

1) Multi-Agent Systems as Dynamic Systems

There is minimal difference between the diagrams in Fig. 6 and the diagrams presented in any number of papers in the literature of multi-agent systems. As such it is natural (at least to a control systems specialist!) to interpret the controllers and the subsystems of the plant as “agents.” While this is not technically correct with respect to the FIPA definitions, this is in fact what has happened in the control systems literature. We can identify three lines of research in which this perspective has been expressed.

a) Large-Scale Systems Theory

We refer again to the 1978 paper [3] and two earlier books [44], [45]. Key aspects of this approach are to look for ways to aggregate subsystems and look for controllers at different levels of aggregation. While the term “agent” does not always appear explicitly in this area, the diagrams are again similar to those found in the HMADS literature.

b) Coordinated/Cooperative/Consensus Control

In this area researchers explicitly use the term agent. The primary focus is on an “agent” that “moves” according to some dynamics (first- or second-order integrators are the most common) and has some form of limited communication with its neighbors. Research has focused on the ability of such systems to reach “consensus,” with respect to some criteria and applications have been demonstrated, most notably for formation flying and other coordinated motion control problems [46]-[48] and in multi-agent systems [32]. Of course, “movement” can be viewed more abstractly than referring simply to physical motion in space and as such the ideas of consensus can be applied more broadly to a wide variety of dynamical systems.

c) Control of Spatially-Distributed Systems

A third category of relevant work is related to the stability analysis and, more recently, the control of systems of distinct components or entities that are considered related but separated in space. These entities are always dynamic systems, usually linear and multivariable, and are interconnected in some way. Initial work in this area concentrated on identical entities and specific topologies of interconnection, but more recent work has extended results to heterogeneous systems and arbitrary topologies (see the extensive work of D’Andrea, represented by [49] and the references therein). Some literature in this area explicitly uses the term “agent,” but most do not.

Note that categories a) and b) above both admit graph-based descriptions. In the next subsection we consider how a graph can be used to model interconnected dynamic systems in a concise way that is amenable to analysis and design. We take as our point of departure the work on consensus coming out of the coordination and cooperative control area and discuss how this work can be extended to the case of dynamic networks.
2) Consensus Networks and their Extensions to Dynamic Networks
   
   a) Consensus Protocols

Suppose that \( N \) agents evolve their individual belief \( \xi_i \) about a so-called global consensus variable, using nearest neighbor communications according to the so-called consensus protocol:

\[
\dot{\xi}_i = -\sum_{j \in N_i} \lambda_{ij} (\xi_i - \xi_j) \tag{7}
\]

where \( N_i \) denotes the neighborhood of agent \( i \). It is easy to represent this as a weighted digraph (directed graph), with a typical interpretation that the agents are integrators and the weights are given by the gains \( \lambda_{ij} \). Next, define a vector of agent variables:

\[
\vec{\xi} = (\xi_1, \ldots, \xi_N)^T
\]

and let \( L = [l_{ij}] \), where \( l_{ij} = \lambda_{ij}, i \neq j \) and \( l_{ii} = -\sum \lambda_{ij} \). \( L \) is called the graph Laplacian and the overall system can be described as \( \dot{\vec{\xi}} = L \vec{\xi} \). A now-classic result that exploits the spectral properties of Laplacians is that if the underlying graph implied by the matrix \( L \) is connected (meaning that there is a least one agent from which there is a path to every other agent), then all the variables \( \xi_i \) will converge to the same value. That is, \( \vec{\xi}_i \to \vec{\xi}^* \) [46]. This is called consensus and Equation (7) is called a consensus protocol. A large amount of research has been carried out on this problem, which can be studied for both digraphs and undirected graphs, for communication protocols that admit delays and higher-order dynamics in the agents, and many more. Also note a key feature of the algorithms in (7). The change in an agent’s belief or estimate of the global variable is a function of the difference between its belief and the collective value of its neighbors’ beliefs. This is an essential point that motivates the thinking in terms of agents in the first place. The idea is that individual actors cooperate according to some predefined rules to come to an agreement. In the following we consider an extension to these ideas to develop what we call a dynamic network. To motivate what follows, note that if we take the Laplace transform of (7) and rearrange terms, we can write the system equations as

\[
(sI - L)\vec{\xi}(s) = 0
\]

b) Consensus Networks with Real Rational Weights

The consensus protocol and its variants have been studied extensively in the literature and have been applied in a number of areas, notably for formation motion control when the agents are mobile. However, the consensus paradigm is restrictive in a number of ways. Notice that we have interpreted the consensus problem as having integrating agents and static weights. One might ask: what if the weights were also transfer functions? What if the agents are more than integrators? In our recent work we have considered this question, motivated by modeling heat transfer in buildings [50].

c) Dynamic Networks

As enumerated in Table 1, one might consider graphs whose agents and interconnections are dynamic systems. Such networks are called “dynamic networks.” Taking a dynamic networks point of view provides a useful way to develop analysis and design techniques for distributed control systems. Emphasized is a goal that “…stability of the entire network must be preserved as this network is modified with the additions/removal of heterogeneous agents, without requiring a centralized analysis each time such a network modification occurs…” and to “…guarantee stability for an arbitrary network, possible structure in the interconnections … become important …”[51]. The point is to exploit the structure of underlying graphs associated with a dynamic network, both for analysis and design.

<table>
<thead>
<tr>
<th>Case</th>
<th>Agents</th>
<th>Arcs (Edges)</th>
<th>Problem Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>No processing</td>
<td>Static arcs</td>
<td>Weighted Laplacian</td>
</tr>
<tr>
<td>2</td>
<td>Integrating Agents</td>
<td>Static arcs</td>
<td>Consensus problem [48]</td>
</tr>
<tr>
<td>3</td>
<td>Integrating Agents</td>
<td>Dynamic arcs</td>
<td>Dynamic Laplacian [48]</td>
</tr>
<tr>
<td>4</td>
<td>Transfer function</td>
<td>Static arcs</td>
<td>Generalized Frequency Variables [22]</td>
</tr>
<tr>
<td>5</td>
<td>Transfer function</td>
<td>Dynamic arcs</td>
<td>New Problem</td>
</tr>
</tbody>
</table>

V. A PROPOSED HMADS FRAMEWORK FOR ANALYSIS AND DESIGN

Consider Fig. 7, which shows, for illustration, a three-layer system, consisting of the computational intelligence-based management and coordination layers, and execution layer with supervisory and local control aspects, and finally the plant environment. Within the management and coordination layers the HMADS framework is achieving what might be expressed as the desired optimal performance, e.g., optimal coordination of assets based upon deconflictions between what the chief executive of a company desires, and what the design physics and regulations will allow. Within the execution and environment layers, what is being attained can be considered the achievable optimal performance, i.e., model-based optimal field device execution to fulfill desires. Note that it is arguable and perhaps only semantics as to whether we call plant components agents or not. But, the extent that both an agent and a subsystem of the plant implement a transfer function, there is no distinction between the two.

In what follows, a notional framework will be provided that considers the practical implementation as a way of contrasting where the suggested research efforts lie. From a management perspective, fuzzy logic presents itself as a methodology to represent policy that is the formulation of input from multiple sources and lacking crispness [52]. For the coordination layer, a BBN provides a mechanism that can represent the historical nature of characterizing normal behavior, and also converting policy into field device action based in a manner allowing feedback [53]. The execution layer is based in the dynamics of
digital control, allowing for the advancement of techniques in consensus theory and other control theory methodologies coupled with fault diagnosis, detection and prognostic methods [2], [47].

In this system we might consider each residence or commercial facility as agents, where voltage and frequency are important considerations in each agent. As the power flows through the system, significant changes in load associated with one agent can affect neighboring agents on the same supply line. With the application of sensors at each agent, voltage and frequency monitoring will occur, providing state awareness at each load. While this awareness can be utilized by a coordination agent to modify generation parameters based upon policy, which will compensate for the disturbance, these dynamics occur rapidly. On the surface this appears to create an added complexity to the multi-agent decomposition, namely the means of monitoring and control are within the same agent as mentioned for a chemical plant earlier in the paper. More specifically, the state awareness data from a load (execution) agent would have to be communicated to the coordination agent at a high speed to ensure a correcting response in generation. If generation were distributed at the execution agent level, some level of control could be directly applied much as with the chemical plant.

Reconsidering the paradigm from the prior paragraph, however, an alternative formulation exists to align the power system with what might be considered the ideal form. To do this requires separation of fast and slow dynamics relative to the HMADS, and a characterization of control response at each layer. Considering a state awareness at the load level, the sharing of peer information between the field device and supervisory control sublayers can be performed (Fig. 7). Within the supervisory controller, which may occur at a substation, the adjustment of capacitance and inductance can be used to provide a level of controllability, (such as with integration of Flexible Alternating Current Transmission Systems (FACTS) used with transmission systems). More aggressive action can occur with demand response, where predefined loads can be taken offline to accommodate higher priority loads. The result of this decomposition is then to establish a performance goal with each that should fall directly, which in this case is to establish power flows to the loads to maintain the appropriate voltage, frequency and phase angle. As part of the management layer, the prioritization of loads would need to be established as an aspect of the policy. In considering how this fits within a fuzzy logic framework, we move from the normalization of how policy is based to the contributions to this policy. Therefore, the development of the management layer fuzzy logic agents is summarized as follows:

- **GIVEN**: Variables established that performance for the plant is based upon.
- **FIND**: Linguistic Variables, Membership Functions and Rule Base.
- **SUCH THAT**: A probability is established that reflects a consensus decision on policy shifts from those in management authority.

The management layer agent for economics of a power system was given as an example in the prior section. Considering now the stability agent for the power system example, there are
three physical variables that affect the dynamics, specifically the voltage, frequency and phase angle. From these variables, the linguistic variables for a fuzzy logic design can then be taken as the basis for the management policy of the HMADS. Typically these variables are fairly uniform across the country, but resilience of the overall system will depend on how closely these variables stay within desired tolerances under upset conditions.

The rule base establishes the constraints on desired operation, including safety, regulatory, economics, etc. While the rule base is established based upon decision of a management authority, current plant documents often codify the current basis for operation. These documents include engineering design documents, operating procedures, regulatory permits, safety basis documents, etc.

Judgments at the management layer are intended to have slower dynamics than the execution layer, but if economic issues such as power market pricing are considered, the potential for a fast dynamic has been introduced. Unlike the consideration of load distribution, market dynamic affects the supplier/buyer of the power commodity and can be a destabilizing force if it impacts management policy. Therefore, while the impacts of change in market prices affect the generation system, the timing for these shifts should occur at the coordination layer (Fig. 5). The coordination layer correlates the policy on efficiency and stability with economics to provide a historically weighed solution.

The output that leaves the management layer is namely the weight to be placed upon a certain type of preference in coordinating resources. For instance, the policy to run certain power plants versus others will normally be based upon economics unless stability or efficiency is affected. Also considering the motivating forces for economic viability by the asset owner, one could easily assume that alignment of resources for marketing purposes will drive most of the dynamics of operation. However, the stability and efficiency of the system must still be maintained, which ensure the cost effective delivery of the power within the expected parameters. Therefore, the output will need to be weighted to ensure stability and efficiency during marketing realignments of generation (and distribution, as affected), which can be correlated to limiting the “stress” placed upon the power system. As a result, the defuzzification system for the management layer establishes a probability parameter that can be used by the coordination layer as a basis for decision, within priorities. An example is allowing constant marketing shifts but limiting impacts on stability.

B. Coordination Layer Framework

As stated previously, the management layer establishes the policy for coordinating the resources under the direction of the HMADS. For the power system, during normal conditions, the primary dynamics are associated with economic shifts of generation. However, during fault conditions that can result from human error, malicious attacks, natural events or emergent behavior, the coordination layer must make adjustments to maintain prioritized loads to achieve resilience. As discussed in early sections, methodologies to recognize and self correct for physical and cyber degradation of sensors and field devices are integrated within the execution layer. However, in developing the BBN for the coordination layer, a historical basis for this conditionality will benefit the apriori
decision making, also providing an aspect of self correction for unexpected, malicious inputs. These subversive inputs may occur at the coordination layer, or originate at the management layer.

A BBN, such as that for a notional power system given in Fig. 5, represents a mechanism to codify relationships between the management and execution layers. However, they also provide a mechanism to represent the development of the historical basis to calculate the probabilities associated with the decisions, where a real time understanding from fused sensor inputs is fed back through the BBN to better characterize the decision space and probabilistic relationships. A next step would be to characterize the necessary Bayesian probabilities associated with the BBN. Therefore, the development of the coordination layer Bayesian is summarized as follows:

- **GIVEN**: Consensus decision on policy provided in terms of $P(H)$ for each management agent.
- **FIND**: The conditional probabilities $P(D|H)$ associated with each of the coordination layer agents.
- **SUCH THAT**: A tasking of the supervisory control agents is established that reflects the current management policy.

Considering the information provided by the management layer, the output of the defuzzification can itself be considered a probability that must be linked, in this case becoming the prior probability of the hypothesis $H$ in Equation (4). That is, the input represents the preference of accepting a particular judgment for realignment based upon the management policy for realigning assets. While Equation (4) represents only one variable, in fact the management policy suggested for the notional power system of Fig. 5 has three, including economics, efficiency and stability. The decisions based on these variables are not mutually exclusive in impacting the alignment of the power system. However, the deconfliction of the coupled effects occurs within the coordination layer as described in the previous section. Therefore, the end result of the BBN is to confirm that the alignment change desired reflects what is actually desired and possible with the execution layer. In addition, it provides historical confirmation that the shift reflects sound, and not malicious, judgment.

The conditional probability reflects what is desired is borne out in maintaining a state awareness of the power system. For the power system stability this feedback can come as the result of state estimation predictors, coupling models with available sensor readings, or directly in the form of synchrophasers or by direct measurement as supplemented with modeling (state estimation). Given these thresholds, the execution layer can then establish target set points for execution agent boundaries. A framework for optimizing the execution layer given the coordination layer tasking is discussed in the next section.

C. Execution and Plant Layer Framework

The execution layer research can be summarized simply as a combination of consensus theory for inter-agent interactions, and conventional control for inter-agent interactions that are associated with the execution layer. This subsection will be specifically focused on the inter-agent interactions, as these are fundamentally critical to the HMADS framework.

Let’s assume that there are transfer functions associated with each interconnected subsystem as well as an interconnection system. (As an aside, it is possible that at the plant level, the dynamics can be such that the plant interconnection matrix is not a Laplacian. In such a case, however, the framework below can still be defined, though the system matrices might have different properties) For the plant, device control, and supervisory control layer, we denote these respectively as $P(s)$, $L_p(s)$, $C(s)$, $L_c(s)$, and $S(s)$, $L_s(s)$. When the execution agents are described by arbitrary transfer functions, not just integrators, we can develop a representation for the supervisory and device control aspects of the execution layer. We do this by defining $P(s)=\text{diag}(P_i(s))$, $C(s)=\text{diag}(C_i(s))$, and $S(s)=\text{diag}(S_i(s))$. Then similar to Equations (7) and (8), if we define vectors of the agent variables for the plant, controller, and supervisors as $X_p(s)$, $X_c(s)$, and $X_s(s)$, then we can describe these systems as

$$[P^{-1}(s) - L_p(s)]X_p(s) = 0$$
$$[C^{-1}(s) - L_c(s)]X_c(s) = 0$$
$$[S^{-1}(s) - L_s(s)]X_s(s) = 0$$

The posterior probability reflects the confirmation that the hypothesis is true, driving the continued realignment of the power system to reflect the policy. This implies that the hypothesis provides what might be considered the control action associated with the coordination layer output to the execution layer, and the Bayesian relationship provides confirmation of the desired state change to achieve this hypothesis. However, the adjustment will occur at a rate that maintains the overall system within the desired constraints for optimal performance, namely economic shifts will still fall within the management policy for efficiency and stability.

Markov modeling of the data sources to establish the conditional probability of the BBN is a common approach [54]. The data sources will need to be correlated to the thresholds established for the coordination agent. For power system stability, voltage, frequency and phase are directly related to power system operation within the execution layer. These are provided by direct measurement using synchrophasers or by direct measurement as supplemented with modeling (state estimation). Given these thresholds, the execution layer can then establish target set points for execution agent boundaries. A framework for optimizing the execution layer given the coordination layer tasking is discussed in the next section.
Equation (9) defines the dynamics of each layer in Fig. 6. Not captured are the interconnections between the layers. To describe these connections, define dynamic links between element $j$ of the plant layer and element $i$ of the controller layer as $\lambda_{CP}(s)$ and weights between controller elements and supervisor elements as $\lambda_{SC}(s)$, with respective Laplacians denoted $L_{CP}(s)$ and $L_{SP}(s)$ (and similarly defining $L_{PC}(s)$ and $L_{PS}(s)$ in the other directions – note that we show directional links between the device control layer and plant layer in Fig. 6, but bi-directional links within and between the control and supervisor layers, depicting the fact that these are usually computer-based communications).

When we combine the interconnections between layers with the relationships that exist on each layer, we obtain the following nested representation:

$$L(s) \begin{bmatrix} X_p(s) \\ X_s(s) \\ X_e(s) \end{bmatrix} = 0$$

(10)

where $L(s)$ is the overall system Laplacian, given by

$$\begin{bmatrix} P^{-1} - L_p - L_{CP} \\ L_{PC} \\ -L_{CS} \\ 0 \end{bmatrix} \begin{bmatrix} C_{-}^{-1} - L_{C} - L_{PC} - L_{CS} \\ -L_{PC} - L_{CS} \\ L_{SC} \\ S^{-1} - L_{S} - L_{SC} \end{bmatrix}$$

The properties of the system matrix $L(s)$ will determine the overall behavior of the system. With this notation, we can define and the following problem for the execution and plant layer:

- **GIVEN:** Plant transfer functions $P(s)$ and $L_p(s)$ for the operating plant, as tasked by the coordination layer.
- **FIND:** The supervisory and device control transfer functions $C(s)$, $L_{CP}(s)$, $S(s)$, $L_{SP}(s)$, $L_{PC}(s)$ and $L_{SC}(s)$.
- **SUCH THAT:** The overall interconnected system defined by $L(s)$ in Equation (10) is stable and meets any specified performance goals.

To solve this problem, the agent layers that describe the execution (supervisory control, device control) and plant layers must first be defined. For the notional BBN breakdown in Fig. 8, this decomposition would include automatic generation and substation supervisory control agents and fuel controls, frequency regulation, etc. for device agents. For the plant, modeled dynamics of the controlled physical system is required, such as the generation plant components, including the turbine, boiler, etc., and substation components and affected loads. Secondly, performance goals need to be defined for the execution and plant layers, which will come in the form of relationships that maintain voltage, frequency and phase within defined constraints. Economic and efficiency tradeoffs of base load generation will be deconflicted at the coordination layer, but the execution agents will be assigned to maintain the desired generation output, and adjustment of power flow to loads. For initial results from the authors regarding plant-controller modeling along the lines of this section, see [50]. For initial results on controller design for H-infinity disturbance attenuation in the setting of this section (execution layer, from a multi-agent perspective), see [55].

Regarding the first solution aspect above, a suitable modeling framework, we believe that work reported in [29] can be brought to bear. This work presents a methodology for giving a global linear systems description of nested hierarchical layers, based on the description of each layer. However, the work does not consider dynamic interconnection links and it assumes homogeneous dynamic systems at each agent. Further research will be needed to overcome these limitations. Additionally, the work does not consider the design problem, but only considers the problem of analyzing a given system for stability.

Regarding the second solution aspect, performance goals, we are particularly interested in identifying relationships between notions of performance and resilience as defined above and ideas from graph theory about effective resistance, minimum “distance” between agents, average number of neighbors, and other graph-theoretic notions, such as how the spectral properties of graphs are affected by its connectivity. We believe the extension of these ideas from the static graphs typically considered in graph theory to the dynamic graphs we have introduced here will be fruitful. Additionally, we point to the behavioral control engineering of Willems [51], [56], which we believe can provide useful analysis tools to be used in this framework.

For the notional BBN breakdown in Fig. 5, the decomposition of the system is dependent upon separation of assets that is logical for minimizing the dynamic complexity of inter-agent interactions. As indicated with the discussion under the management and coordination layers, the loads uniquely identified with each substation indicate one instantiation of this breakdown. Within the substation, certain loads will be critical and given priority over other loads in providing control actions to maintain voltage, frequency and phase. As inputs from the coordination layer provide the basis for supervisory control actions transmitted to the execution layer, the supervisory layer will need to translate these into field device actions. Considering the consensus problem, the ultimate goal is to stabilize the inter-agent dynamics. Therefore, the weights between supervisory and device control layers will need to codify this interaction in terms of establishing control actions or set points within the execution layer in one direction, and feedback in the other that capture the desired behavior. In simple terms, the decision to adjust reactivity to affect the total power factor or shed a load is a control, and sensor information of voltage, frequency and phase is a feedback to ensure desired results. Where renewable generation is present, control actions can include adjustment of offsets between load requirements, storage recharge and available bulk power availability. More regional corrective actions, including bulk power system generation, could be imagined based on the
inability to achieve results while recognizing a particular substation has a critical load.

VI. SUMMARY

What has been presented is the development of a notional HMADS framework to model distributed control system dynamics, and in doing so, achieve resilience. Resilience is achieved in the replacement of many human interactions with a structure that establishes management policy, coordinates assets, and operates the assets based upon the BDI of the management authority. In providing this framework, a research strategy is outlined for methods that can be used to attain global performance. This step forward is necessary, as the tailoring of this framework to multiple critical infrastructure applications will be necessary before the common precepts of a standardizable design strategy are codified.

Applied at the management and coordination layers are methods that can be used to provide consensus and codification of event-based dynamics that are typically characterized by human input. For the execution layer, time-based dynamics that traditionally characterize a control system are tied to the global strategy. However, consensus is also a key aspect of this layer. To ensure the resilience of the overall framework, recognition techniques at both the event-based and time-based layers are implemented to ensure degradation is recognized. Within the execution layer, promising techniques are referenced. This will require extending the framework above and in [57] to include noise, disturbances, and robustness considerations. Within the HMADS, the Bayesian design of the coordination layer provides a means of ensuring a historic norm is established to provide this recognition.

VII. ACKNOWLEDGEMENT

Work supported by the U.S. Department of Energy under DOE Idaho Operations Office Contract DE-AC07-05ID14517, performed as part of the Instrumentation, Control, and Intelligent Systems (ICIS) Distinctive Signature of Idaho National Laboratory. The authors would like to express their appreciation to Ray Grosshans of the Center for Advanced Energy Studies for his timely reviews and recommendations that benefited the quality of this paper.

REFERENCES

information,” 1st International Conference on High Confidence Networked Systems, pp. 1-10, April 2012.


