High Assurance Smart Grid: 
Smart Grid Control Systems Communications Architecture

Thomas M. Overman, CISSP, ISSMP, PMP
Chief Architect, Boeing Energy Cyber Security
Boeing Defense, Space and Security
884 Hermosa Ct.
Sunnyvale, CA 94088
thomas.overman@boeing.com

Ronald W. Sackman
Chief Network Architect, Applied Network Solutions
Boeing Defense, Space and Security
884 Hermosa Ct.
Sunnyvale, CA 94088
ronald.w.sackman@boeing.com

Abstract—As increasing numbers of “smart” sensors and actuators are introduced into the electrical grid, the cyber security factor grows in significance, necessitating the implementation of information assurance controls for devices at all levels within the grid communications network. Determining the appropriate controls for any particular device first requires identifying its place within an established trust model. This paper aims to define a multilevel framework for a trust model to be used throughout the electrical grid.

Assume compromise of control systems – A primary objective in developing this model is to support a distributed rather than hierarchical control system architecture based on the core assumption that the compromise of grid control system components and subsystems will always be to some extent unavoidable. Rather, therefore, than attempting to create an all-encompassing enclave of trust, our control system architectural model suggests that systems be designed in ways to narrow the sphere of implied trust by expecting the compromise of adjacent systems, thereby reducing the sphere of vulnerability. By starting with an expectation of control system component compromise or lack of trust, subsystem designs can be implemented with independent rather than dependent cyber security and energy control data flows.

The term High Assurance Smart Grid (HASG) refers to a Smart Grid with a control system architecture characterized by a distributed architecture that is designed to mitigate against widespread failures when control system components themselves are compromised. Lessons-learned and best practices are adopted from power engineering, information technology, cyber security, and other disciplines to build the described HASG model.

Keywords-Smart Grid; Trust Model; Standards; Cyber Security; Information Assurance

I. INTRODUCTION

The electrical grid encompasses everything from large-scale power generating facilities, through transmission and distribution systems, to building management systems (BMSs), home area networks (HANs), and various electrical loads connected to the system. It also includes both centralized and distributed power generation and storage systems that vary in scale by several orders of magnitude. The grid can be viewed as a networked system of systems with literally millions of nodes.

For many years there have been reports of cyber security vulnerabilities being identified and exploited within the grid, and as “smart” electronic sensors and actuators proliferate over the coming decades, implementing appropriate cyber security controls will become ever more critical to overall system health. Given such an extensive and diverse system of systems, it is neither possible nor necessary to establish peer trust relationships between every network device. For example, a home water heater and a transmission substation actuator have very different impacts on the overall grid.

Drawing upon insights to be gained from an unrelated field but one in which reliable networked system of systems operations are of critical importance, we may borrow an important design principle from avionics systems engineering: Aeronautical systems must be designed such that the failure of adjacent systems is expected, i.e., each system and subsystem is implemented in a way that precludes the failure of an associated subsystem from producing cascading malfunctions across a wide number of networked systems. From a Smart Grid cyber security perspective then, rather than attempting to create an all-encompassing enclave of trust, our model suggests that systems should be designed in ways that anticipate the compromise of adjacent systems, whether through system failure, user error, or malicious activity.

A number of other network safeguards, taken together, can be implemented to enhance security for grid control systems. Information technology (IT) best practices combine several cyber security systems—firewalls, role based access control (RBAC) functionality, malicious software protection systems, encryption of data at rest and data in transit, and host/network intrusion detection systems to name just a few. All of these and more are necessary parts of modern control system architecture.

There have been significant writings over the past few years about cyber security threats to grid control systems, with many authors expressing the firm belief that the threats they discuss—from nation-state actors, to cyber terrorists, to sophisticated criminal organizations—are very real and tangible. Use of defense-in-depth methodologies is thus a necessary part of any serious effort to protect grid control systems. However, even a robust combination of such systems is not sufficient for today’s, much less for tomorrow’s, increasingly complex control systems.
In reality, the addition of hundreds, thousands, and potentially millions of additional grid sensors and actuators will have the advantage of providing grid operators with substantially improved fidelity of status and control over electrical grids. However, these modern sensors and actuators are more complex than their electromechanical predecessors; and increased complexity at both the individual device level and the overall system level inherently introduces more fragility than with the traditional electromechanical controls. While there are many examples of fully functional grid actuators that have been in service 40 or more years, many electronic control system components have not been in existence for even a small fraction of that time span. Consequently there is no real service life history (as opposed to test-based projections) to demonstrate that the new technologies will have the same reliable service life as traditional systems.

The fragility of the new grid devices, the possibility of cyber attack, or the inadvertent action of potentially untrained or distracted employees increase the likelihood of unplanned outages to the control system components themselves. When these factors are added to the well known grid vulnerabilities from unplanned line outages, higher than expected loads, and loss of generation capacity, HASS reliability challenges are further increased. The widespread introduction of intermittent generation sources will also exacerbate this situation. Rather than positing an unsolvable problem, however, this combination of traditional and new vulnerabilities offers an opportunity to rethink the underlying architecture of the grid control systems themselves.

II. GRID CONTROL ARCHITECTURE

Before addressing the details of the HASS model, it may be well to recognize that there are at least two distinct definitions for the term “high assurance.” One, taken from the System Engineering discipline, characterizes a high assurance system as being reliable, available, safe, secure, and timely. Another definition is related to formal evaluation assurance levels EAL-6 and EAL-7. In our view, rather than being competing definitions, the EAL approach can be seen as a subset of the broader field of High Assurance System Engineering.

The original power distribution grid itself implemented a hierarchical radial or hub and spoke footprint. As transmission systems came online, these too initially implemented the same topology. The modern grid includes hundreds of large scale generators within each interconnect and serves hundreds of thousands of large industrial customers and millions of commercial and residential customers. Over the years, most transmission and some distribution operators have increased system reliability by introducing numerous interconnects between various intermediate nodes. These interties provide redundant paths between generators and loads. Some of this redundancy provides increased capacity, and some of the redundancy is purely for reliability purposes, so that should a primary link fail, there is an alternate link already installed. This redundancy can reduce both the frequency and duration of outages.

For purposes of this discussion we depict the power grid as a greatly simplified tree structure, Figure 1, which compares the characteristics of the past hierarchical energy flow with the present interconnected energy distribution scheme.

![Figure 1 Simplified Past and Present Energy Flow Tree Comparison](image1)

These simplified diagrams show how energy flow has been managed in various parts of the transmission and distribution grid for many years. It is interesting to note, however, that while the power flow grid is more interconnected and less hierarchical at present, the energy control system architecture, Figure 2, still maintains a centralized, hierarchical data flow between control room, substations, and field devices.

![Figure 2 Hierarchical Grid Control Data Flow Network](image2)

Grid devices have three basic modes: manual control, automatic control, and remote control. (There is also a data load or maintenance mode, which is outside the scope of this paper.) Manually actuated devices need no further description. Automatic devices, as defined here, are primarily self-preservation devices. These and similar devices combine a local sensor and an actuator, often in a single unit. Automatic circuit breakers are a classic example of an entirely automatic device. Automatic reclosers are another such device. While more sophisticated than circuit breakers, automatic reclosers are also predominately electromechanical devices that make a fixed number of attempts to reclose an electrical circuit in order to reenergize the affected line. Neither manual nor automatic devices, as defined here, are the subject of interest for this paper. Remotely controllable sensors and actuators are of primary interest for this discussion.

The control network depicted above (Figure 2) is based on the electrical grid of the past (left-hand portion of Figure 1). It reflects the control data flow in a primarily hierarchical manner, where field device control is subordinate to the relevant substation, and where substations are subordinate to control room data flows. In this model, which is typical of most control
room environments known to the authors, there is little if any peer communication or autonomous coordination between field devices, or between one substation and another. Each field device and substation has essentially automatic modes of operation in which decisions are executed in a fairly binary manner and can be made based entirely on the state of local sensors.

While substations and field devices in such a hierarchical scheme can and do make locally preprogrammed actions, decisions requiring higher complexity or broader grid considerations are typically beyond the capacity of these devices. For decisions beyond self-preservation (such as tripping circuit breakers), or for actions by devices such as automatic reclosers,[5],[6],[7] substations to some extent—and field devices almost exclusively—rely on receiving commands from higher-echelon control rooms. Thus, while electrical power flow within the grid is far more interconnected than in past years, the control system data flow is still predominately hierarchical, with most energy control today still based on a model related to the original grid built 100 years ago. Herein lies the challenge and the opportunity as we build a “Smart Grid” for the future.

Figure 3 shows the combination of grid interties already widely implemented, with increased coordination between intelligent electrical devices (IEDs) in a manner not entirely dependent on control room input. In this new control system architectural model, field devices have some ability to sense peer devices beyond their traditional world view. Substations have the ability to collaborate across wider areas, again, without the requirement for this communication and control signaling to be done exclusively through control rooms.

![Figure 3 Interconnected Grid and Grid Control](image)

It is noteworthy that the proposed architecture makes no attempt to eliminate lines of communications and control data flow between field devices, substations, and control rooms. Instead, the focus is on enhancing the distributed control signaling architecture such that some level of device collaboration can be performed even when there are losses of control capability from the still dominant hierarchical control system architecture.

The loss of reliable control capability may arise from a wide variety of failure modes. Among them

1. Communications link failure,
2. Sensor and/or actuator controller failure,
3. Unplanned control center system failure, and
4. Nonexistent, late, or improper commands by untrained and/or distracted control room personnel.

It should be noted here that rather than characterize malicious activity as a separate category, the first three listed failure modes could be caused either by inadvertent/unplanned hardware/software failures, or by malicious activity initiated by disgruntled employees or external attackers. That concept is central to the recommended approach which sees focusing cyber security efforts just on preventing external attack as insufficient.

For this paper, “loss of reliable control” is assumed to be caused by any of the enumerated failure modes. While it is true that some failure modes result in complete loss of control and others result in loss of reliable control, we make no distinction between these nuanced definitions and will use the term “loss of reliable control” throughout our discussion.

Key to the proposed architectural model is that all sources of failure are addressed without recourse to extensive and sometimes distracting discussions about the likelihood of failure caused by an external attacker. In reality, the goal of most external attackers is to gain insider access. Thus if the control system architecture can limit damage caused by untrained and/or distracted utility personnel, or by the unplanned control link or control system outages, it will be inherently more resilient against attack by malicious actors.

The U.S. Department of Energy has long promoted the goal of an “autonomous, self-healing grid.”[8],[9] While it is unlikely there will ever be a truly autonomous and self-healing grid that manages itself independent of any human-in-the-loop (HITL) control system, striving toward this goal has significant benefits from a cyber security perspective.

Analyses of the 2003 Northeast blackout, 2008 Florida blackout, and other such events show that many widespread outages occur without any evidence of malicious activity involvement. Instead, these outages occurred because of a combination of factors which could be anticipated. Four primary causes were involved in the Northeast 2003 blackout:[10]

1. Inadequate system understanding.
2. Inadequate tree trimming resulted in multiple 345-kV and 138-kV transmission lines failing when they sagged into vegetation.
3. Control system and communications failures at the operating utility did not give control room operators sufficient visibility to the outages within their territory.
4. A concurrent control system failure and inadequate data feeds at the Reliability Coordinator did not allow their operators sufficient visibility to the transmission failures within the transmission operator’s territory.

Had the operators at the local utility and the regional balancing authority retained visibility to the current state of the transmission grid, it has been stated that the blackout likely would not have occurred. This is because normal control room system functionality was still available that would have enabled...
grid operators to determine the appropriate next steps to route power around the failed transmission line.

It is entirely appropriate to place significant focus on control system reliability as a means to decrease the likelihood of similar occurrences in the future, but if that is all that is done, then grid sensors and actuators will still be entirely reliant on receiving the next set of instructions from a hierarchical control room. In addition to increasing the reliability of the control systems themselves, distributed grid sensors and actuators must be given either more autonomous capability or, at a minimum, a preloading of next steps to be taken in case of a variety of failure modes. In order for this to be effective, it is also imperative that distributed sensors and actuators gain the ability to have a wider world view than just sensing their immediate surroundings and sending data up/down a hierarchical control flow.

The Report of the 2003 Blackout lists, “Violation 1: Following the outage of the Chamberlin-Harding 345-kV line, [the transmission line operator] did not take the necessary actions to return the system to a safe operating state within 30 minutes.”[11] There are, of course, multiple ways to avoid this situation in the future. The most common approach is to increase the reliability of the sensor/actuator network and of the control room systems themselves, together with enhanced training for control room operators. This, however, misses a key point: control room systems and control data links are likely to fail again, and whichever failure mode causes a loss of reliable control is relatively immaterial. Whether due to inadvertent failure, error, oversight, or malicious action, the loss of reliable control should be planned for, with mitigation features being built into distributed actuators in the grid.

These authors submit that in addition to the four primary causes of the 2003 northeast blackout shown in [10], there is a fifth primary cause:

5. The hierarchical nature of the control system architecture was such that when the initial transmission line failed due to contact with vegetation, field devices alerted the control room and waited for instructions as to what remedial action to take.

The design flaw to be corrected lies in the very hierarchical nature of the control system itself.

From a practical perspective, it would likely be infeasible to have all grid devices preloaded with corrective actions for all possible failures. The IEEE 39-bus system, as shown in Dynamics and Control of Large Electric Power Systems (Figure 13.35)[12] demonstrates this quite well. In this figure, there are 10 generators, 39 buses, and 51 links. Even if the only failure mode were complete failure of any link or node (an open circuit), there would be 100 failure modes. In reality, there are many times that number, because there are more failure modes than open circuits (e.g., current, frequency, and voltage variations), and there is the high likelihood during congested periods of having more than one simultaneous failure. Of course, not all failure modes are equal. Many grid devices are sufficiently isolated from one another, and there is no requirement for all devices to be able to compensate for all failure modes.

III. Trust Model Considerations

As stated earlier, establishing an all-encompassing sphere of trust for Smart Grid controls is neither possible nor desirable. This is true whether considered on a regional/national basis or an individual utility basis. In addition to distributing communications and decision-making capability, control room, substation and field devices must have the ability to sense when to trust—and when not to trust—received sensor and command input. This is a particularly challenging area but one well worth considering.

Compromise must be assumed in grid control systems. In addition to the assumption of outright failure (missing data), this section is more explicitly about incorrect sensor and command information, whether inadvertent or malicious in nature. Much research and development has been done in the areas of intrusion prevention systems (IPS) and intrusion detection systems (IDS). In part this is because components to solve problems in this area are definable, and commercialization of such system components is fairly straightforward. We are not suggesting that the overall problem is simple, but that IPS and IDS component systems are well definable, and therefore a variety of vendors have developed solutions in this area.

Fault-tolerant systems have long been researched and engineered. System redundancies and failover systems are examples. Intrusion-tolerant systems (ITS) are the subject of a related but newer field of research. There are a number of papers addressing this, among them K. Meng et al and F. Gong et al[13],[14]. The concept of an ITS approach is that while implementation of IPS and IDS systems is important, quite often these systems prove ineffective at preventing system intrusions. Security systems occasionally fail to perform their intended functions for a variety of reasons.

Perhaps more important, a focus on just IPS and IDS systems fails to account for failure modes caused by distracted or untrained insiders. It also fails to account for insiders with malicious intent. An ITS, however, can account for these failure modes. As a general approach, addressing the insider threat (whether error- or malice-driven) has significant merit. It accommodates failures of IPS and IDS, and it focuses on what an outside attacker generally attempts anyway, i.e., to gain insider privileges. An ITS focus also addresses the fact that unpredictable people are already within whatever sphere of trust could be built.

For the electrical grid, a non-ITS approach is shown in Figure 4. Most of interest for this discussion is that the substation or field device has implicit trust in the commands received from the control room. The sensors transmit information to the control room, the control room systems (or the operator) determine whether or not to close the switch, and the switch closes when instructed to do so. In this case, the power on the two sides of the switch is out of phase. Still, the actuator works off blind trust that the command received from the SCADA control system is a reasonable command. The Aurora Generator Test conducted by Idaho National Lab demonstrated that quite effectively.[15] There was nothing particularly “magical” about the attack. The attackers just issued commands for the generator to connect to the grid out of phase. Since the controller on the generator had no ability to synthesize sensor data—which
would have told it the power was out of phase—it merely did what it was told. This resulted in its destruction. While there is good work coming from that test in the area of increasing the security capabilities of the control infrastructure, there is little being done to increase the ability of field devices to sense for themselves whether command inputs received are reasonable to execute.

Figure 4 Traditional Hierarchical View of Grid Control

The better model for the electrical grid control systems is for the substation and field devices to have the ability to independently validate the reasonableness of commands received and to do so in a way well beyond self-preservation tests. In this view, Figure 5, the remote sensors still communicate with the control room, and the control room still sends commands to the remote actuators. The distinction in this view is that there is sufficient distributed intelligence for the remote devices to synthesize information from distributed sensors and from the control room in order to determine whether or not to actuate.

Figure 5 High Assurance Smart Grid Control

This method compensates for malicious commands, for erroneous instructions sent by the untrained or distracted control room operator, and for nonexistent commands as may happen when there is a failure of the control systems themselves. It is this latter part which has the most significance for moving toward the goal of an “autonomous, self-healing grid” spoken of in section III. An architecture which gives substation and field devices the ability to validate not only the integrity but also the reasonableness of commands received also produces an architecture where devices can have a wider world view than just self-preservation activities. It is from there that the first steps can be taken in prepopulating devices with a subset of the results of “What If” analyses. This also represents the control system architecture that will be needed in order to create more autonomy and self-healing capabilities for the grid—not just for individual grid devices.

IV. CONCLUSIONS

There is no single solution to Smart Grid cyber security. It is only through the application of a combination of approaches that grid control systems can be sufficiently engineered for both the electric reliability already expected and the cyber security implications of emerging sensor and actuator technologies.

Current grid control systems are in large part designed in such a way that when a failure occurs, that event is communicated to a control room, and the field devices wait to be told what to do next. A fundamentally different approach would be to distribute the decision-making ability to the substation and/or field devices, or at a minimum, to preload these distributed devices with sufficient information such that they can take automatic (if not autonomous) action in the event of a system failure without having to wait for instructions from the control room. Even without waiting for the technological advances required for full autonomy, preloading substation and field devices with a set of next-actions-to-be-taken instructions, when coupled with a distributed rather than hierarchical communications architecture, can significantly increase grid reliability while simultaneously reducing real-time impact from loss of reliable control.

In the final analysis the best way to increase the reliability of the electrical grid is to use a multi-tier impact-based approach to determining device/system criticality, implement a robust defense-in-depth strategy, and still maintain the assumption that grid control systems will for a variety of reasons be compromised—then engineer for the assumed compromise by transitioning from a hierarchical grid control architecture to a distributed grid control architecture.

V. AREAS FOR FURTHER RESEARCH

There is no expectation that the full complexity of transmission or distribution control room state estimators and other applications will be miniaturized and installed on single-board computers of substation and field devices. However, there is a significant amount of research and development work in the areas of autonomous robotics and multi-agent coordination which provide examples for how grid devices can work with limited individual capability and yet manage,
together, more complex operations than any individual device could do on its own. In addition, further research in the area of ITSSs in the electrical or other control systems environments could have significant value.

VI. REFERENCES

[19] The Boeing trusted software center at the University of Illinois at Urbana-Champaign. http://www.itl.illinois.edu/content/boeing-trusted-software-center.