



HOW TO SAVE AGING ASSETS

Applying limited resources to critical infrastructure

BY MASSOUD AMIN, IEEE Smart Grid, University of Minnesota

The Smart Grid's contributions to improving electric utilities' means of monitoring the condition of assets, providing enhanced situational awareness, and faster actionable intelligence have transformed the power industry's concept of asset management from a largely passive, time-based approach to a more proactive, condition-based assessment.

Condition-based asset management offers a big leap in accuracy, improved and, therefore, greater power grid reliability, as it is a sounder method for asset maintain/repair/replace strategies and related investments. Unfortunately, this "new" approach remains wholly inadequate to meet the challenge.

As the Smart Grid has evolved, so has the need for a much more robust and wide-ranging view of the critical nature of our power infrastructure and how to best manage it. Currently, condition-based asset management is simply one aspect of a more holistic quality management approach that weighs the relative risks and economics of asset maintenance, repair, and replacement to advance end-to-end power grid reliability, resilience, security, and modernization.

This holistic approach will require new, strategic alliances between the public and private sectors in which carrots are used more often than sticks. Moreover, it will require utilities to transform their cultures and organizations and, possibly, adopt new business models to monetize new services and achieve savings.

A FUNDAMENTAL SHIFT

Why should we turn to this more ambitious approach? Simply put, the electric power sector is uniquely foundational to every sector of our economy and quality of life. Virtually every crucial economic and social function in modern society depends on the secure, reliable delivery of electric energy, thus the urgent need for best

practices in the operation of power and energy infrastructures. With a largely aging power infrastructure in the United States—particularly underground city networks—and limited resources to address the issue, we need a rational, evidence-based foundation for its operational integrity and security.

Trends such as urbanization, the power grid's interdependencies with other infrastructures (for example, water, gas, telecommunications) the extreme weather events that come with global climate change and the advent of terrorism all bring added urgency to our collective challenge.

The approach outlined in this feature is based on the familiar trio of technology, policy, and standards, but it also embraces a completely new outlook by all stakeholders towards our power infrastructure. Therefore, this feature closely reflects a report that an IEEE Joint Task Force provided to the U.S. Department of Energy (DOE) in the summer of 2014 on high priority issues for the White House's Quadrennial Energy Review (QER) to guide U.S. energy policy.

A GROWING NEED

In the U.S., the average system age is 40 to 60 years old. Fully 25 percent of our power assets are of an age in which condition is a concern. Power infrastructure build-outs in the U.S. largely ended in the 1980s. Moreover, according to the recently published book, "*Aging Power Delivery Infrastructures*", the current focus is on the maintenance and modernization of existing infrastructure, and maintenance needs alone are expected to double over the next two decades.



A Lawrence Berkeley National Laboratory study has estimated the economic losses of unreliable electricity in the U.S. to be approximately \$80 billion per year, but other estimates place it as high as \$130 billion per year, not including power quality events. A report by the Electric Power Research Institute (EPRI) and the U.S. Department of Energy has estimated the cost of electricity outages at \$125 to \$188 billion per year with weather accounting for about \$18 to \$33 billion of that amount.

These weather-related costs fluctuate significantly and are greatest in the years of major storms, when they induce economic losses in the range of \$40 to \$75 billion, according to the U.S. Energy Information Administration.

Obviously, massive investments are needed to address aging power infrastructure, reliability and hardening improvements, Smart Grid-related technologies, the interdependency of electricity- and natural gas-related assets and cyber and physical security. As an electric system ages, operating costs increase and reliability decreases. Utilities possess limited resources for wholesale replacement of infrastructure, thus the emphasis on managing

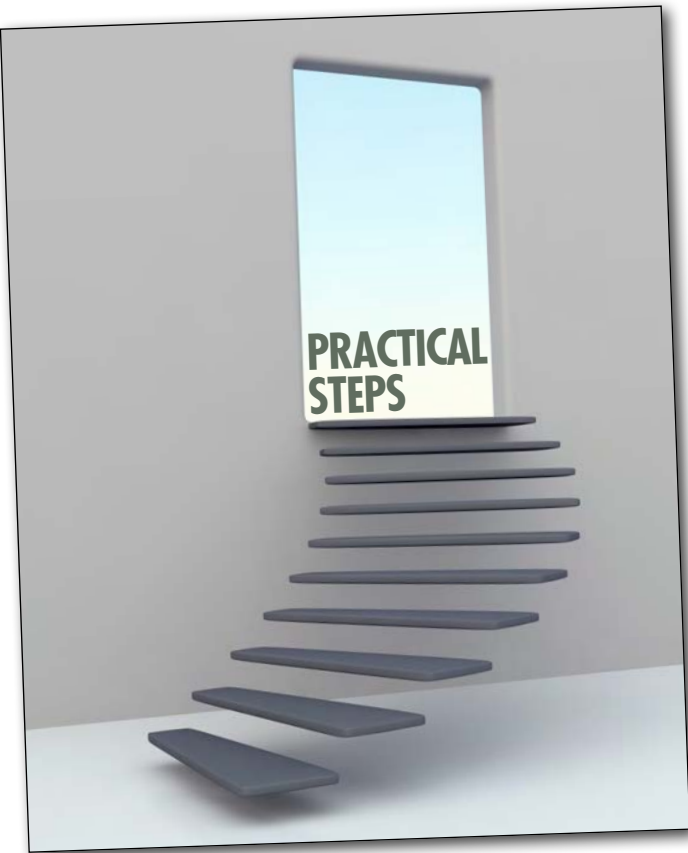
assets in a holistic manner.

Every utility will need to develop sound strategies for controlling the symptoms of aging within the utility's overall business plan, while maintaining accepted levels of performance. A holistic asset management approach is attractive in that it provides predictability, both in terms of meeting acceptable reliability indices and cost constraints.

A utility's capital and operations and maintenance (O&M) budgets must address the triad of system capability and reliability, aging infrastructure and grid hardening for vulnerable elements. Thus, an approach that properly assesses risk in each of these three major areas and directs capital and O&M investments within the framework of a utility's business plan is both efficient and effective.

Of course, the interdependencies within a utility organization require coordination. Consequently, a holistic asset management approach is bound to have implications for cultural transformations within and between a utility's historically siloed departments, as well as for the power grid itself.





PRACTICAL STEPS

Achieving hardening and resiliency on the ground should be based on a particular utility’s customers’ needs, its legacy systems, location, and technology roadmap. Given the disparities between individual utilities, it is difficult to generalize, but a few universal concepts are worth discussion. Never forget that “resiliency” and “customers’ needs” also cover the timely notification, through customers’ preferred channels, of estimated time to restoration, which increases customer satisfaction.

Risk assessment of existing assets provides a data-based identification of weaknesses and a means of prioritizing maintenance, repair and replacement. Component and system failures are difficult to predict. However, it is possible to identify the components that, as a result of their location, configuration and electrical characteristics, pose the greatest risk for large-scale outages. Understanding these vulnerabilities can guide power grid investments.

Because the risk landscape is dynamic, risk assessment must be a perennial task. Additionally, adaptation strategies will shift as a utility invests in new technologies and operational practices change. Current and future investments in advanced metering infrastructure and distribution automation signal the beginning of a multi-decade, multi-billion-dollar effort to achieve an intelligent, secure, resilient, and self-healing system. The risk landscape will change as the power grid evolves.

Fortunately, risk assessment methods are well established, and they can be tailored to specific circumstances. Three figures offer insights related to this task. Figure 1, from the National Institute of Standards and Technology (NIST), provides a conceptual model for enterprise risk management.

Figure 2 is based on an adaptation of Dr. Steve Lee’s work at EPRI on probabilistic risk assessment (PRA) as a part of the EPRI Grid Operations and Planning Task Force’s Power Delivery Reliability Initiative, and my published works entitled, “Fast Look-ahead Simulation, Modelling and Validation, January 2001 to May 2003”.

NIST: Enterprise-Wide Risk Management

- Multi-tiered Risk Management Approach
- Implemented by the Risk Executive Function
- Enterprise Architecture and SDLC Focus
- Flexible and Agile Implementation

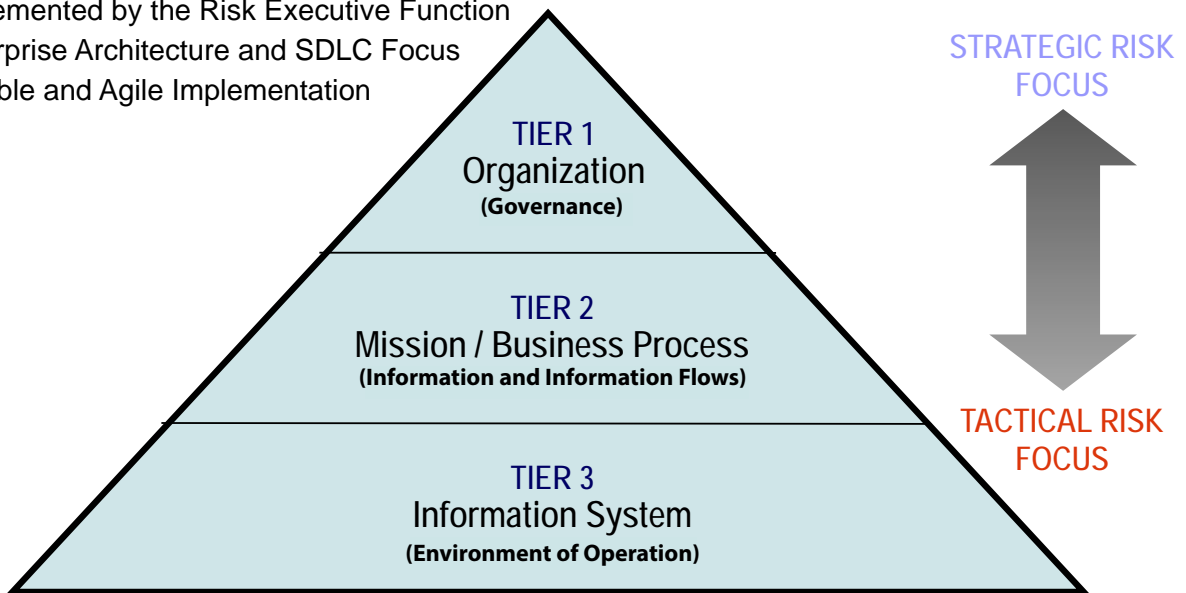
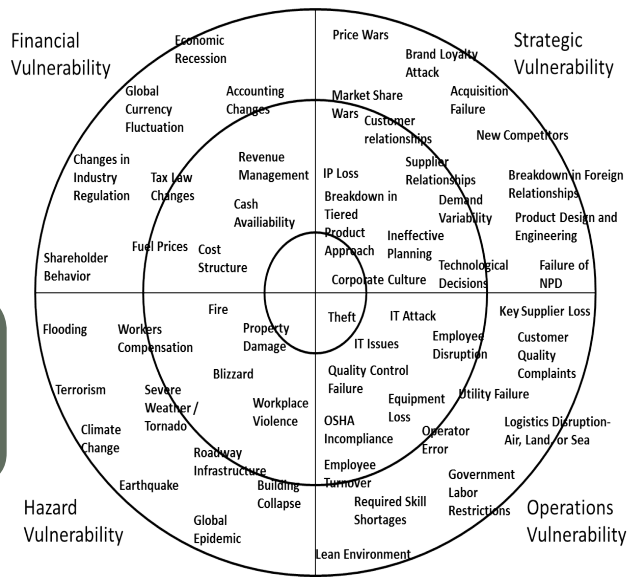


Figure 1

Enterprise risk management (conceptual model)
Source: National Institute of Standards and Technology (NIST)

Approach

- **Vulnerability mapping**



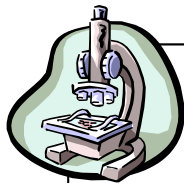
- **Scenario analysis**

- **The green movement**
 - Resilience requirement for new suppliers
- **Middle East embargo**
 - New projects require improved delivery
- **Non-renewable energy abundance**
 - Supplier and product distribution will provide snapshot of product portfolio health

Figure 2

This illustration provides a target-and-crosshairs model for vulnerability mapping to prioritize risk factors across four sectors, including operational, hazard, financial and strategic vulnerabilities

Example of In Depth Analysis: Critical Contingency Situations



Critical Root Causes in the Proba/Voltage Impact State space (Region Cause: all, Affected Region: all)

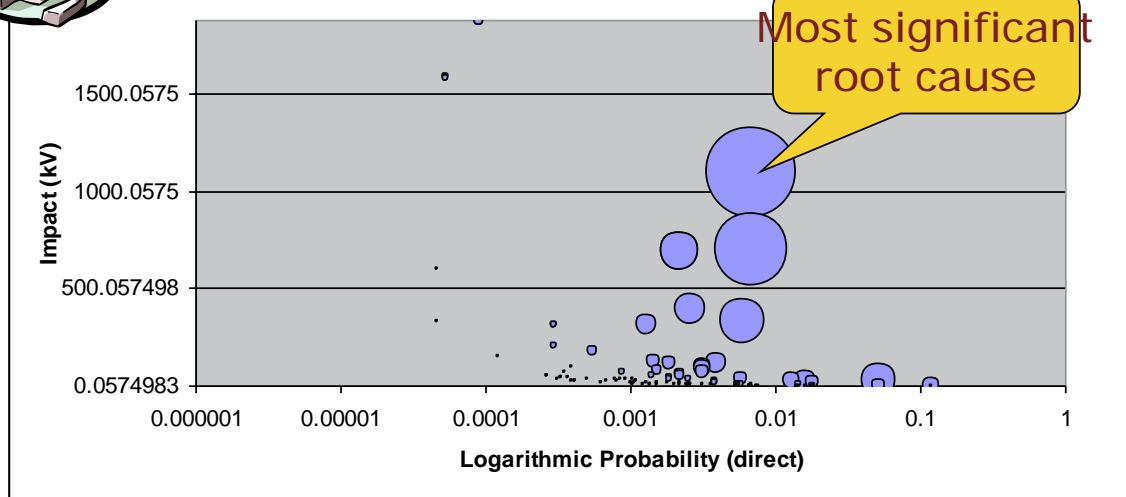


Figure 3

Illustration of how probability and voltage factors can be combined to determine high-priority investments; It is taken from the author's work on adopting the methods discussed in Professor Yossi Sheffi's book, "The Resilient Enterprise", for a holistic risk assessment/asset management tool for utility decision-makers

ELECTRIC-GAS INTERDEPENDENCIES

A holistic view of assets must include the increasing interdependency of electric power and natural gas. As more power plants shift to natural gas-driven generation and play a role in balancing the variability of renewable energy and demand-side programs, natural gas plants and their fuel supplies will become a critical asset to monitor for condition and performance.

The issue goes beyond existing facilities to supply capacity. In some areas of the U.S., particularly in winter, unsubscribed capacity on gas pipelines is becoming rare. Thus, new gas pipeline capacity, as well as existing pipeline conditions, has become tied to power reliability.



CYBER- & PHYSICAL SECURITY

In a holistic approach, the security of assets is fundamental. Asset condition is of little consequence if the component or system in question has been manipulated or rendered inoperable through a physical- or cyber-attack. Yet the sheer size, complexity and evolving threat landscape for power infrastructure presents daunting challenges.

Transmission and distribution system assets sprawl largely out in the open, unless they disappear under city streets. The increasing sophistication and proliferation of sensors and actuators (combined in IEDs) and related data networks and reliance on public communication networks and Internet protocol (IP) means that cyber-attack vectors have proliferated, too.

The physical security of field assets appears straightforward, but evolving cyber-physical interdependencies such as information and communication technologies (ICT) need to be addressed. The dropping cost of physical surveillance tools such as video cameras and motion detectors will offer opportunities to bolster physical security solutions (also known as “physec”).

Cyber threats are dynamic, evolve quickly, and can exploit utility staff inexperience and lack of training. In fact, instilling a security-minded culture among utility staff can be the greatest challenge. Cyber connectivity has increased the complexity of the control system and the facilities under control. Thus, significant challenges must be overcome before extensive deployment and implementation of Smart Grid technologies, which may introduce new vulnerabilities. The overall strategy relies on security measures being “baked in” to devices and systems and the application of a layered, “defense in depth” approach.



CONDITION MONITORING

Condition-based monitoring of assets is preferable to a reactive, “fix-on-fail” approach, which can be dangerous and costly to end users, and it will remain a pillar of a holistic asset management approach for the near future. Integrating condition and operational data, in fact, can yield insights into real-time system operations in terms of asset use as well as the strategic replacement of failing assets.

Keep it simple. A proliferation of unneeded sensors can overload the user with too much data and create unmanageable complexities. The strategic deployment of basic sensors plus existing intelligent electronic devices, or IEDs (for example, protective relays), may provide sufficient information for condition-based maintenance as well as aiding situational awareness, in turn leading to reduced outage propagation and improved responses to disturbances. Condition-based monitoring raises questions (refer to “Condition Monitoring Questions” sidebar); a holistic asset management approach can lead to answers.

CONDITION MONITORING QUESTIONS

- 1
How will the utility obtain spare components, if a device fails?
- 2
What is the data-based justification for a planned replacement?
- 3
How can a utility improve its purchase specifications and achieve greener operations?
- 4
What are effective approaches to education and training for a workforce that rarely encounters the assets in question?



WHAT ASSETS TO PROTECT

Fuel supply and generation assets: A “successful” attack (that is, one that produces widespread or long-term interruption of power) on generation assets is likely to have a local or regional rather than a national impact, because of these assets’ redundant nature.

Transmission and distribution assets: Transmission lines (especially those linking areas of the power grid), key substations and switchyards, control centers and distribution feeders to major urban areas need protection. Assessing the response time for recovery, particularly for long lead-time equipment, should be explored.

Controls and communications assets: Widespread, coordinated denial of control and communication systems could cause significant disruption, particularly in SCADA systems, communications between control systems, monitoring systems, and business networks.

Many factors impede the protection of assets, including the inability to share information between federal, state, and local authorities on threats, vulnerabilities, and protection strategies. Federal statutes such as the Freedom of Information Act (FOIA) impede such information sharing. The challenge is to define sensitive information and access requirements to facilitate security without allowing public access.

Other impediments include cost, widely dispersed assets, owners and operators, training and empowering security personnel, the use of commercial off-the-shelf (COTS) controls and communications, siting constraints, and long lead times on replacement equipment.

Many Federal statutes impede information sharing between levels of government

IDENTIFYING NECESSARY STANDARDS

The IEEE Standards Association has developed and approved standards pertaining to the assessment of aging infrastructure as well as power grid security.

Nuclear Facilities

IEEE Standard 1205: “*Guide for Assessing, Monitoring, and Mitigating Aging Effects on Electrical Equipment Used in Nuclear Power Generating Stations and Other Nuclear Facilities*” provides guidelines for assessing, monitoring, and mitigating the effects of aging on electrical equipment used in nuclear power-related facilities. This guide includes insights on aging mechanisms, environmental and condition monitoring.

Electrical Substations

The IEEE Power and Energy Society (PES) Substation Committee on Aging Infrastructure and Resiliency has developed a number of pertinent standards, including the 2014 edition of IEEE 1402: “*Guide for Electric Power Substation Physical and Electronic Security*”. The existing 1402-2000 standard establishes minimum requirements and practices for power substations’ physical security during construction, operation and maintenance, as well as methods and designs to mitigate intrusions.

The new P1402 scope is broader and addresses a number of threats, including unauthorized access to substation facilities, theft of material, and vandalism. Additionally, the new P1402 scope establishes requirements for different levels of substation physical security.


Intelligent Electronic Devices

IEEE 1686: “*Standard for Intelligent Electronic Devices (IEDs) Cybersecurity Capabilities*” defines the functions and features to be provided in substation IEDs to accommodate critical infrastructure protection programs by addressing IED access, operation, configuration, firmware revision, and data retrieval.

Other Substation Standards

In related work, IEEE working groups are developing standard 1646: “*Requirement and Application of the Substation Cybersecurity*”. The scope for this new specification includes technical requirements for substation cybersecurity and the standard presents sound engineering practices for cybersecurity of automation, protection, and control systems.

Additionally, IEEE has developed a working group to address standard 1711: “*Trial-Use Standard for a Cryptographic Protocol for Cybersecurity of Substation Serial Links*” to define a cryptographic protocol to provide



integrity and optional confidentiality for cybersecurity of substation serial links. One IEEE working group is addressing issues within the published current edition of 1711, while the other address an alternate approach to a serial encryption protocol developed under the Pacific Northwest National Laboratory (PNNL) called the Secure SCADA Communications Protocol (SSCP).

Power System Communications

IEEE working groups are currently revising the 2012 edition of IEEE 1815: “*Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3)*”. This revision is important because DNP3 Secure Authentication was significantly improved from the version listed in the IEEE 1815-2010 specification. The version included in Clause 7 of IEEE 1815-2010 is identified as SAV2 (Secure Authentication v2), and the version included in Clause 7 of IEEE 1815-2012 is identified as SAV5 (Secure Authentication v5). The two versions are not compatible and must be aligned.

An assigned working group is making advancements in the IEEE project called P2030.102.1: “*Standard for Interoperability of Internet Protocol Security (IPsec) Utilized within Utility Control Systems*”. This new standard creates a

profile to support interoperability in the deployment of Internet Protocol security (IPsec) to secure utility communications.

THE UTILITY CHALLENGE

Every utility has a unique customer base, business model and legacy system and its own interests at stake in providing reliable, affordable power while promoting resiliency in the face of myriad vulnerabilities. Asset management can be accomplished with incremental steps. Urgent needs might take a year. Tactical shifts might require two to three years. Strategic goals may take three or more years.

Collectively, however, we must recognize that every utility’s efforts contribute to the quality of life, economic stability and, thus, the security of our nation. For that reason, the IEEE Joint Task Force on priority issues in the White House’s Quadrennial Energy Review made recommendations on what role the federal government might play in support of state and local efforts to aid power and integrated utilities in increasing reliability, resilience, and security.

In the U.S., the average system age is 40 to 60 years old. At the moment, 25 percent of America’s power assets are of an age in which condition is a concern.

MACRO-RECOMMENDATIONS

Increased federal research and development for emerging technologies to improve the reliability, efficiency, and management of the power grid includes new types of generation and energy storage. Documenting best practices on the deployment and integration of new technologies would be welcome.

Overlapping and inconsistent roles and authorities of federal agencies can hinder development of productive, public-private working relationships, thus a new model for these relationships is required for infrastructure security.

For instance, a stockpiling authority, be it private or governmental, could obtain long lead-time equipment based on the power industry's inventory of critical equipment, which must include the number and location of available spares and the level of interchangeability between sites and companies. Clearly, further standardization of equipment will reduce lead times and increase the interchangeability of critical equipment.

A perennial entry in power industry recommendations to the federal government is to provide alternatives for utilities that wish to avoid wireless telecom networks and the public Internet to decrease power grid vulnerabilities by, for instance, enabling utilities to obtain private spectrum at a reasonable cost.

Improving the sharing of intelligence and threat information and analysis to develop proactive protection strategies might include the development of threat coordination centers at local, regional, and national levels.

Perhaps all these measures could be facilitated by more transparent, participatory, and collaborative discussion among federal and state agencies, transmission and distribution asset owners, regional transmission operators, and independent system operators and their members to improve stakeholders' understanding of mutual interactions, impacts, and benefits. **ET**

Massoud Amin is a senior member of IEEE, chairman of the IEEE Smart Grid, a fellow of ASME, and professor of Electrical and Computer Engineering at the University of Minnesota.

Related Articles



The 2015 Asset Management Plan

STATE OF INDUSTRY