CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

STRATEGIC TECHNOLOGIES PROGRAM

October 2015

The Case for Simplicity in Energy Infrastructure

For Economic and National Security

Michael Assante, Tim Roxey, and Andy Bochman

To disrupt today's nation state adversaries and tomorrow's cyber terrorists and hacktivists, we must reengineer selected last-mile and endpoint elements of the grid. This activity need not be applied to every system on the grid, rather, only to those we judge most essential to national security. But we need to begin this process now.

Accepting the Truth

In 2015, if we weren't so busy modernizing the North American grid and keeping it patched and protected, we might have noticed something that could have changed outcomes considerably. Before you read further, recall the scene from the film *The Matrix* where Neo is given a choice between accessing the harsh ground truth in the form of a red pill or maintaining the current comforting illusion with a blue one. He opts for red, and the plot unfolds. So proceed with caution: this brief is a red pill, and once read, you will never see grid cybersecurity problems or today's so-called solutions the same way again. Ready?

Dispatch from the Near Future

We gave ourselves a self-inflicted wound. We were running at full speed to try and keep up. We observed this, enumerated that, and captured lists of increasingly more vulnerabilities to address, threats to protect against, problems to mitigate, and weaknesses to understand and shore up. We were always finding additional challenges to chase on this treadmill and had ourselves convinced we were doing all the right things. The price we bore for all that running? Escalating costs, high and ever-increasing complexity, more regulation, more oversight, more uncertainty, and more risk. Meanwhile our adversaries, operating on an entirely different level, built multiple powerful tools to defeat each of our clever new solutions. Easily overmatching us, they clearly beat us at this game. For far better than we knew ourselves, they fully understood our systems, our networks, our people, and the interdependencies among them. In short, they got us right where they wanted us, and in a very real sense, we were totally complicit.

Simple Origins: Complex Results

The old analog relays and circuit protection devices were as reliable as the day was long. But they are now being replaced by computer-based devices with more memory and processing horsepower than the utilities' first mainframes had. Once simple, these machines are now being accessorized with modern technology to help them play their part in new information technology (IT)–oriented "smart" environments (e.g., grids, plants, cities, etc.) that we are building out as fast as we can. Although these modern technology enhancements will result in greater productivity and efficiency contributing trillions of new value to the global economy, we are also unlocking an equally powerful dark side that can negate these advantages.

For every large physical machine that makes, manages or moves electricity (e.g., natural gas generators, voltage step-down transformers) hundreds of digital devices have evolved to support them. Remote terminal units (RTUs), intelligent electronic devices (IEDs), programmable logic controllers (PLCs), distributed control systems (DCSs), field programmable gate arrays (FPGAs): these are specialized computers with circuit boards, memory chips, and communications circuits, the parts sourced from innumerable suppliers, and animated via instructions coded in software. And while the hardware brings loads of complexity, it's in software that complexity truly runs wild. One need merely glance on occasion at MITRE Corporations' growing list of common vulnerabilities and exposures (CVEs) and common weakness enumerations (CWEs) or sample the latest security bulletins from the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) to appreciate that we're drowning.

Mix in a whorl of oversight organizations, legislation, regulatory frameworks, standards, and continually changing guidance, and we've baked ourselves a layer cake of complexity and abstraction that no one in their right mind would want. At each layer in each domain (physical, technological, human, and regulatory), one finds expanding attack surfaces and enough vulnerabilities to provide lifetime employment to armies of researchers. Then, consider that these unpredictable elements interact in ways so complex they can never be fully comprehended by us, let alone fully accounted for or protected.

Against this gathering storm of complexity, we find regulatory regimes providing demonstrable risk reduction. Best known, perhaps, are the continuously improving North American Electric Reliability Corporation (NERC) critical infrastructure protection (CIP) standards, which require ever more stringent cyber (and now physical) security controls for utilities operating bulk electric system elements. Also noteworthy are the emerging Nuclear Regulatory Commission (NRC) orders. It's only through the determined efforts of many dedicated people, corporations, and regulators that the regulatory frameworks developed and deployed in the nuclear and broader electric sector have had such a marked impact on improving the overall level of cyber hygiene of the grid.

Alas, we know that good hygiene is necessary to thwart the majority of nontargeted attacks, but it is not sufficient when it comes to targeted attacks by determined adversaries with enormous resources and the highest competencies at their disposal. The most advanced threat actors can and often do bypass the many prescribed controls used in our defenses. So the takeaway is that while it is imperative that we continually invest in better hygiene to remove entire groups of threat actors, we have to acknowledge that: (1) there is a limit to what we can prevent, and (2) we must prepare for adversaries equipped to gain access to our most critical systems.

Armed with this knowledge, we can begin to turn the tide decisively to our advantage by engineering targets off the table. One key concept in this effort is: don't over digitize. Another is: obfuscate high-priority targets. Relying on a strategy that depends solely on hygiene will win many battles, but without additional steps, we risk defeat in the most important ones.

Calculating the Costs of This Complexity

Unless one's a wine maker or novelist, complexity is not a desirable attribute. In the grid, it's an unintended byproduct that's been created by our push to do more and do it faster, cheaper, with more precision, with fewer people, and at greater distances. Up to a certain point, we can handle it; it's not very noticeable, and it causes little additional risk to operations. But a handful of folks are waking up, like Neo, to the fact that our most important systems are increasingly inhabited by and under the control of external actors. Mounting complexity and our own acceptance of it are the primary accomplices.

As we know from other domains, there is a point of diminishing returns where more energy is required to sustain the complexity than the complex system provides in benefits; and in the electric sector, we're well past that point. Complexity contributes absolutely nothing to make the grid more reliable, and the accumulating costs are neither reasonable nor acceptable, nor from a national security perspective, tolerable.

1. We pay first because we pay directly for every layer of complexity we create.

2. We pay a second time because these layers are petri dishes for the growth of new attack surfaces and new interdependencies, which are not understood but can—and have—contributed to additional negative consequences.

3. We pay again because our development work teaches our savvy and attentive enemies.

4. We pay yet again because the layers consume our intellectual interest, talent, financial resources, and workforce availability that could have been used to perform other, obviously higher value, activities.

5. Finally, we pay when an error is made or a system is mis-operated and we experience disruption and loss.

Many electric utility security programs and professionals are already fraying around the edges, with most running full speed just to stand still. How these teams will handle a concerted series of medium-to-long duration targeted attacks on critical systems is very much in question. These questions have already resulted in a confidence crisis with policymakers that may result in a more widespread public confidence crisis and a "digital backlash."

Advantage: Attackers

As we've made it easy for them, attacker sophistication should be viewed first through the lens of intent. Disrupting or hijacking system resources is one thing; destroying trust and confidence by poisoning data is another; massive exfiltration as a precursor to advanced analysis of ICS system and network chokepoints is yet another. Initially protected in large part by isolation, control systems are now increasingly interconnected. The defenses for them have not evolved nearly as quickly as those used to guard corporate IT; in fact, most are a full decade behind the current levels of exploit technology, and the gap is only growing. Of course, attackers know and delight in this. And because we show no signs of getting off the complexity treadmill we've created (or even acknowledging it exists), they can bank on the fact that things are only going to get better for them in the future.

Unless, that is, we do something radical—upset the business-as-usual apple cart and bring transformational change to selected parts of this vitally important enterprise. We need to look beyond treating the problem to changing the rules of the game itself.

The Path Back from Complexity

For our nation's sake, we can begin to bound this seemingly overwhelming problem by first understanding what we are trying to avoid and acknowledging that we can't fix everything. And fortunately, we don't need to. If we narrow our vision and set our sights on the comparatively small number of systems that MUST, from a national security perspective, be kept safe, we already have the process and technology means at our disposal to take back control.

It's Simple

First, if we are to achieve a defensible grid, we must put each layer of complexity to the test. To do this, we'll have to gauge whether the layers in question (physical, technological, human, and regulatory) deliver business and system risk-reduction value commensurate with the level of effort expended to maintain it, while we grapple with the ripple effects of the complexities it induces.

A quick look at just the regulatory layer, for example, finds utilities in 2015 operating on a playing field strewn with standards, policies, guidelines, compliance audits, and the regulatory and oversight organizations that enable them. A not nearly exhaustive list for just the electricity subsector would include the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF) and NISTIR 7628, the Department of Energy's (DOE) electricity subsector cybersecurity capability maturity model (ES-C2M2) and risk management process

(RMP), innumerable standards promulgated by industry technical groups, the torrent of security alerts and bulletins from the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) and ICS-CERT, and of course, the mandatory security requirements for reliability of the high-voltage bulk electric system: the NERC CIPS. On the distribution grid, where electricity is actually delivered to end users including cities, companies, DoD bases, etc., state public utility commissions (PUC) own responsibility for active oversight of cyber activities of utilities.

One doesn't need a crystal ball, however, to imagine that most of the other layers won't pass muster either. In which case, we should pursue an abnegation (or functionality pruning) approach, such as recently described by former secretary of the navy Richard Danzig:

> Pursue a strategy that self-consciously sacrifices some cyber benefits in order to ensure greater security for key systems on which security depends .... Determining the trade-offs between operational loss and security gain through abnegating choices will require and reward the development of a new breed of civilian policymakers, managers and military officers able to understand both domains.[1]

Development of professionals with the right hybrid mix of skills is now underway, but it's going to take a much bigger push to grow the numbers needed to see this plan through. In fact, in part to counter our infatuation with technology and technological fixes, we have some major investments in human capital ahead of us.

Back to Basics

Grid operations are increasingly automated and tightly coupled, forcing more and more humans out of the decisionmaking process loop. Of course, that only makes a thorough understanding of the automated processes all the more important. The drive to simplify requires that we isolate and understand the essentials of what we ask our automation and control systems to do. The following four areas all link to a data-driven and risk-informed systemic-level grid understanding:

- *Control.* Control includes elements that mediate generator functions like pumps and valves and that step and offer voltage, frequency, capacitance, and current under various load conditions. It's composed of technologies that govern and enhance power quality, reactive power balance, coupling of asynchronous systems, and stability management over long transmission distances, as well as short-circuit incidence reduction in meshed systems. Control speaks to power provisioning for dynamic market requirements and demand response, and the provision of base observables for operator machine interface readings and alarms.

[1] Richard J. Danzig, *Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies* (Washington, DC: Center for a New American Security, July 2014), 6, http://www.cnas.org/sites/default/files/publications-pdf/CNAS_PoisonedFruit_Danzig_0.pdf.

- *Local System Awareness*. For the most important nodes, operating status information proximate to key points of critical control must be accurate and based on real-time science and grid status. Today, utilities often receive status data that's been transmitted, reflected, or recreated over distance from pathways reliant on intermediate processing, undermining confidence in what they see.

- *Self-sustainability*. We ask our control systems to operate reliably and efficiently at remote sites and offer appropriate fail-safe assurances, grid redundancy, segmentation, and sustainability on operational and cost efficiency levels. This reliable and efficient operation happens best when the components involved are not too complex, are durable, and can be installed and repaired with relative ease, all of which lessen the need for remote access and interaction.

- *Update Capability*. When intervention is required, one design feature worthy of pursuit is the ease with which updates to capabilities, settings, and configurations can be made. To the extent that control system elements can be updated with moderate effort, and as long as a trusted human is in the loop, a number of benefits are conferred upon asset owners, including increased reliability and performance.

In addition to pursuing simplicity, we need to remove the opportunity for our adversaries to enumerate and control vital devices. Along these lines, we introduce a new term that will become common as these efforts continue: attack surface interruption (ASI) zones. We can use analog, nondigital, or purpose-built digital circuits that act as ASI zones to thwart attackers. One method would be to insert analog boards between IEDs or other ICS endpoints and the digital control network. It's a retro approach guaranteed to stymie even the most sophisticated cyber adversaries, who, if they're really intent on achieving a specific objective, will have to physically touch the equipment. When we force them out into the open, we can deal with them on our own terms. We won't stop them from attacking, but we can reduce their impacts while ensuring that their attempts don't go undetected.

Go Back to Go Forward

In the late 1970s TV show *Battlestar Galactica*, humans, having migrated to outer space, find their ships devastated by a hostile series of cyber attacks, with only one spaceship surviving. The outdated destroyer, *Battlestar Galactica*, last in line for the fleet-wide upgrade to digital controls, proves to be immune to cyber attacks and lives to fight another day.

Like the famed *Battlestar*, industrial control systems were entirely analog in their original incarnations. In most U.S. nuclear power plants today, analog safety systems are still the norm. However, a seemingly inexorable fleet-wide digital upgrade is underway, and despite knowing in our bones that we're adding complexity, uncertainty, and cyber risk to our nuclear plants, absent a better way of thinking, most seem resigned to this fate.

When considering the risks and rewards of going fully digital in the most critical of critical infrastructure systems, the optimal solution will often be a hybrid architecture where the benefits of digital are realized while the determinism of analog is drawn upon as an impermeable bulwark of cyber defense.

Breathing Room

Attackers always come in a range of capabilities with a variety of objectives. To date we've been defending, with some success, against hygiene-level threats using the tools our security industry has built for us and regulatory levers for reliability like the NERC CIPS to ensure a common security floor is in place in the bulk power system. However, while improving the sector's reliability and performance against lower level cyber threats, these tools and standards have less efficacy in terms of protecting our electric infrastructure from the most determined, most capable, targeted attackers. And despite the high potential impacts on some areas like the grid's rapidly evolving lower voltage distribution system and the high-value infrastructure elements that plug into it (e.g., DoD facilities, critical manufacturing facilities, other critical commercial and industrial users, etc.), there are no standards and little guidance on how to protect these against advanced adversaries.

We don't have to remove all complexity—there's no point in even trying. But in order to disrupt today's nation state adversaries and tomorrow's hacktivists, we've got to reengineer selected elements of the grid. These techniques need not be applied to every system on the grid, rather, only to those we judge most essential to national and economic security. Meanwhile, as business interests have strong economic incentives to continue treating the symptoms (vs. solving the core problem), the already well-established engine of incremental security improvements will continue to roll on, addressing hygiene-level challenges and making profits for suppliers attempting to address the ever-expanding universe of lower-risk threats.

But businesses—utilities and suppliers alike—can and must be part of the ultimate solution. In order to enlist their efforts, we'll need to do several things. We'll first have to make them aware of the stakes, using vivid scenarios that reveal their level of involvement and the extent to which their interests align with the nation's. We'll need to develop credible metrics they can understand to baseline and track progress as these efforts begin in earnest. We'll also want to create appropriate incentives to motivate and rapidly propel the behaviors we need, including investment strategies that prioritize thorough protection of the absolutely most critical processes and assets.

One thing's for certain: the current approach to grid protection works well for reliability but will not stop skilled, adaptive adversaries, for whom our current methods virtually guarantee success. It's time to wake up and face this reality head on. Now that you've ingested the red pill, for the sake of the U.S. grid on which so much depends, please join us in changing the game.

Acknowledgments

This report is made possible by general support to CSIS. No direct sponsorship contributed to its publication.

About the Authors

Michael Assante is a senior associate with the Strategic Technologies Program at the Center for Strategic and International Studies (CSIS) in Washington, D.C. Tim Roxey is vice president at the North American Electric Reliability Corporation (NERC) and chief operating officer of the Electricity Information Sharing and Analysis Center (E-ISAC) in Washington, D.C. Andy Bochman is senior cyber and energy security strategist for the Idaho National Lab (INL) in Idaho Falls, ID.

This report is produced by the Center for Strategic and International Studies (CSIS), a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).