*Science and Public Policy*, 46(3), 2019, 339–346
doi: 10.1093/scipol/scy061
Advance Access Publication Date: 15 November 2018
Article

OXFORD

# Regulating risks within complex sociotechnical systems: Evidence from critical infrastructure cybersecurity standards

**Aaron Clark-Ginsberg[1,2,*] and Rebecca Slayton[3]**

[1]Stanford University, Stanford, CA, USA; [2]The RAND Corporation, Arlington, VA, USA; and [3]Cornell University, Ithaca, NY, USA

*Corresponding author. Email: clarkginsberga@gmail.com

## Abstract

Using regulations to reduce risks in complex systems is controversial, with some arguing that regulations are ineffective, while others argue that they are essential even if imperfect. In this article, we show how regulations and the systems that they aim to regulate function together as a complex sociotechnical system that influences risk management. We first argue that regulatory influence is shaped by three factors—incentives, scope, and adaptability—which are a product of the interactions between the regulations and the system they regulate. Next, we assess the effect of one set of regulations, the North American Electric Reliability Corporation's Critical Infrastructure Protection standards, on the cybersecurity risks faced by the US electric grid. Our assessment shows that the regulations reduced many but not all cybersecurity risks, and at times may have worsened them. We argue that regulatory influence should be understood as *emergent* from interactions between regulations and the systems that they regulate.

**Key words:** cybersecurity; critical infrastructure; regulations; risk management; complexity; emergence.

## 1. Introduction

Technologically-developed nations depend on many complex systems, including the Internet, hospitals, the electric grid, the environment, and transportation networks. Unexpected interactions are a common feature of these systems, which unfortunately can sometimes lead to nuclear meltdowns, oil spills, airplane crashes, extreme floods, and other catastrophes (Perrow 1984, 2007; Sagan 1993). Governments have created regulations—legally binding rules or directives maintained by an authority—to incentivise risk mitigation. However, there is wide disagreement about just what kinds of regulation are best for managing the risks of complex systems, and whether regulation is even an effective mitigation tool.

In this article, we analyse regulation as part of a dynamic sociotechnical system that involves interactions between many stakeholders, regulations, and physical systems. Drawing on original empirical research, we identify three related aspects of regulation which are shaped by these interactions: *incentives*, *scope*, and *adaptability*. We argue that the effectiveness of regulation in achieving its goals is shaped by these aspects of regulation as they emerge from the interactions between formal regulations and complex systems. Our approach builds on science and technology studies (STS) scholarship that shows how large systems intertwine social, political, and technological processes, often in unexpected ways (Bijker et al. 1987; Hecht 1998, 2001; Hughes 1983).

We also draw upon the relational turn in sociology, which emphasises that order emerges somewhat unexpectedly from interactions in complex systems, and cannot always be predicted in advance (Padgett and Powell 2012). Sociologists have argued that risks in complex systems are similarly emergent, evolving as a by-product of collective actions (Centeno et al. 2015; Le Coze 2005). Here we build on these observations by arguing that the effects of regulation should also be understood as emergent—that is, as a somewhat unpredictable outcome of interactions between regulators, organisations that are regulated, auditors, complementary industries, and so on.

This approach is consistent with recent calls to understand policy influence from a complex systems perspective. For example, scholars have argued that research policy (Sen 2014) and immigration policy (Hart 2007) should be considered from a complex systems perspective. However, this approach is less common in studies of regulation; state regulation is typically seen as an external influence that impacts a complex system, often in negative and unintended ways.

In what follows, we first briefly review the debate over the regulation of complex sociotechnical systems, focusing on arguments about the effectiveness of regulatory incentives, scope, and adaptability. Secondly, we provide a detailed case study that

systematically assesses the influence of regulation in each of these areas. Specifically, we analyse the influence of the US Critical Infrastructure Protection (CIP) standards, which aim to lower the risks of a cyberattack on the bulk electric system, one of the most complex sociotechnical systems in the world. Our analysis is based on original interview-based and observational research conducted in 2016, including nearly seventy interviews of regulators, auditors, engineers, consultants, and other stakeholders involved in the CIP standards. This approach is consistent with scholarship that has emphasised the relational nature of infrastructure; what for one group is a transparent and taken-for-granted system, requires various forms of work by those who continually maintain and repair it (Bowker and Star 2000; Lampland and Star 2009; Star and Ruhleder 1996; Star 1999).

As we discuss in the concluding section, the regulations have succeeded in reducing the risks of this extraordinarily complex system, often through unintended and emergent interactions between regulation and the physical and social features of the infrastructure. We argue that since all complex systems can be understood from this sociotechnical perspective, system-level emergence is particularly pertinent part of the influence of regulations, and can be accounted for by designing regulations to incorporate the operational concept of resilience.

## 2. Regulation in complex systems

Complex industries such as petroleum production, civil aviation, and nuclear power produce 'public risks' which are widely distributed and temporally remote and thus tend to be ignored by the risk producers (Huber 1985: 74). Efforts to reduce such risks often seek to focus regulatory resources on the largest risks, as determined by formal risk assessments (Demeritt et al. 2015; Hood et al. 2001). However, in complex systems, many risks are difficult to measure empirically because they involve rare but highly consequential events (Shreve and Kelman 2014). Many risks are also difficult to predict because of uncertainties intrinsic to complex systems (Himmelsbach 2017), resulting in debates about the appropriate level of regulatory precaution (McLean and Patterson 2012). Many policymakers and scholars have instead advocated various forms of 'self-regulation' (Ayres and Braithwaite 1992; Braithwaite 1982; Coglianese and Mendelson 2010; Rees 1988) or 'process-oriented regulation' (Gilad 2010; May 2007; Shohet 1996), in which industries are held accountable for implementing certain kinds of processes (such as planning and self-auditing), but are given considerable autonomy in designing those processes.

Evaluations of self-regulation are conflicting. Some argue that risk-based regulation is fundamentally inappropriate for complex systems, and that too many public goods are sacrificed in the interests of avoiding remote risks (Wildavsky 1988). Others favour regulation but acknowledge that system components can interact in nonlinear ways, creating risks and disaster cascades that are impossible to fully predict (Clark-Ginsberg et al. 2018; Perrow 1984; Pescaroli and Alexander 2015). Tools like regulations will inevitably fail to stop all interactions that create risk, and can sometimes result in even larger disasters than those created if interactions were allowed to occur unabated (Taleb and Blyth 2011; Wildavsky 1988). Complexity means that resilience—the ability to rapidly respond, recover, adapt to, and transform in response to emerging risks and disasters—becomes the cornerstone of the risk management process (Manyena 2006). By contrast, others argue that, far from being antithetical to risk management, regulations are important tools for managing risks in complex systems, both because complex systems contain many predictable risks which regulations are well-suited to address and because regulations can be designed in ways that foster resilience to unpredictable hazards (Macrae 2010; Perrow 2015). Most, however, contend that effectiveness is highly contextual, varying based on the specific properties of regulations and the systems that they regulate (Coglianese et al. 2003; Hood et al. 2001).

A STS perspective can shed light on the relationship between regulations and the systems that they regulate. STS conceptualises science, technology, and regulation as mutually influential components in a seamless web (Downer 2010; Jasanoff 1990, 2005; Wetmore 2004). Regulations are part of a sociotechnical system that both reflects and enacts political and social structures, shaping physical infrastructure in ways that empower certain stakeholders or experts (Busch 2011; Hecht 2001; Hirsh 1999; Hughes 1983; Hughes 1987). Thus, it is essential to examine how regulations interact with the rest of the sociotechnical system, including the new risks, opportunities, and relations that emerge from those interactions. Three aspects of regulation stand out in this regard: *incentives*, *scope*, and *adaptability*.

### 2.1 Incentives

First, many scholars have argued that regulation creates *incentives* for private actors to provide public goods, such as safety and the protection of vulnerable populations, rather than sacrificing those goods for economic gain (Perrow 2015). However, others argue that regulations may produce unexpected perverse incentives (Grabosky 1995; Sunstein 1990), particularly in complex systems. The incentives created by regulation are hard to predict in such systems because they are contingent on a host of interacting institutional, organisational, and social factors (Busch 2011; Star and Lampland 2009). Contrary to the notion that organisational culture can be engineered by supplying appropriate regulatory incentives (O'Neil 2011; O'Neil and Krane 2012; Weick and Sutcliffe 2011), sociologists emphasise that culture is complex, emergent, and difficult to instil centrally through rational measures (Silbey 2009; Vaughan 1999). Additionally, regulations are themselves structures, which can exacerbate complexity and unpredictability and heighten the chances for failures (Busch 2011; Vaughan 1989). Potential for failure can be further compounded by regulators' reliance on industry experts and knowledge, particularly for complex technologies, enabling regulatory 'capture' (Demeritt et al. 2015; Downer 2010; Gormley 1986; Haines 2011; May 2007).

### 2.2 Scope

Secondly, regulations can mitigate systemic risks that fall out of the *scope* of individual private sector actors. For example, regulations can help actors to identify systemic risks by requiring them to share information, and can ensure prudent investments are made in mitigation and other risk reduction activities (Macrae 2010). Regulations allow infrastructure operators to rest assured that their partners in neighbouring infrastructure sectors will maintain certain thresholds of reliability (Schulman and Roe 2016). However, the *scope* of regulations may still be too narrow to mitigate risks which emerge from complex and highly interconnected systems, because these transcend the boundaries of institutional structures (Ansell et al. 2010; Boin 2009a,b; Centeno et al. 2015). In general, regulations designed to limit one type of risk have the potential to increase other risks which may be out of regulatory scope (Macrae 2010;

Vaughan 1989; Weick and Sutcliffe 2011). For instance, regulations designed to improve security in the airline industry can overlap with and hamper airline safety processes (Pettersen and Bjørnskau 2015). Tensions like these are inherent to complex sociotechnical systems, and are part of the reason it is not possible to fully eliminate risk (Schulman and Roe 2016; Turner and Pidgeon 1997).

### 2.3 Adaptability

Thirdly, regulations can help complex industries prepare for and *adapt* to changing social needs or unexpected problems. Adaptability refers to both how regulations enable the system to adapt to changing conditions and how regulations adapt to changing risks. Adaptability is important because sociotechnical systems have emergent properties that are difficult to predict. The work of regulation can contribute to adaptation by helping to institutionalise certain safety practices and reflective thinking among individuals in regulated organisations (Macrae 2010), but can also dis-incentivise information sharing by penalising regulated entities for failures. Furthermore, while regulations themselves must be adaptive, developing appropriate regulations for complex sociotechnical systems can be very time-consuming and politically controversial, meaning that standard setting processes can sometimes fail to keep up with changes (Eisner 2017). Regulations can also create a false sense of certainty or safety, which can limit the ability to discern emerging changes, respond or adapt to processes, or react to emerging crisis (Abraham and Sheppard 1999; McGoey 2007).

## 3. The influence of the North American Electric Reliability Corporation CIP standards

Here we assess the effectiveness of North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) standards in reducing the risks (both probability and impact) of a cyberattack on the bulk electric system (BES), which includes electricity generation and transmission, but not distribution. The CIP standards apply to all computers that could impact the reliability of generation facilities and transmission substations, and enforcement using spot audits began in 2009 (FERC 2008). While a cyberattack has not caused a blackout in the United States, there is reason to believe that cyberattacks are a real threat to the reliability of the electric grid. The Northeast blackout of 2003—one of the largest blackouts in the world and a catalyst for developing the CIP standards—was partially caused by a software failure (U.S.-Canada Power System Outage Task Force 2004) and cyberattacks have been used to compromise power systems in Ukraine in both 2015 and 2016 (Department of Homeland Security 2015).

The CIP standards consist of thirty-two requirements within eleven standards, and cover issues such as personnel and training, electronic and physical security perimeters, and incident reporting and response. Assets within the scope of the standards are classified as low, medium, or highly critical, with more protections required for highly critical assets and fewer for less critical. Regulators, auditors, engineers, and consultants described the CIP standards as a 'start', a 'baseline', and a 'floor', offering a minimum amount of protection but not enough to stop a determined adversary. They fit within a process-oriented regulatory regime, as organisations are held accountable for implementing certain security controls for their assets, but the specific controls required depend on the assets' level of risk, and organisations have discretion to assess their own risk.

By their very design, the CIP standards foster a complex set of interactions between regulators and regulated entities. The Federal Energy Regulatory Commission (FERC) has designated NERC, a non-profit organisation managed by the industry, with developing and implementing the standards. NERC develops the standards through a standards development team comprised of industry volunteers. Once developed, industry votes to approve or reject the standard. If a super-majority approves the standard, the standard then goes to FERC, which can approve, approve with modifications, or remand the standard. Eight regional groups within NERC (often called 'coordinating councils') enforce the standards for all utilities and other regulated organisations within their geographic areas. If they find violations during audits they can fine utilities as much as $1,000,000 per day per violation. The standards are modified continually and are currently in their sixth iteration. Although the CIP standards do not aim at complexity per se, the need to foster interactions between these many stakeholders inevitably creates complexity.

The standards are a potent test case for examining how regulations affect risks in complex systems. The US bulk electric system is an extraordinarily complex system which is critical to the well-being of every segment of American society, but which could nonetheless fail catastrophically. Spanning the country and interconnected with the electric grids of Canada and Mexico, it is comprised of dozens of governmental bodies, over 3,000 small and large public and private utilities, 5,800 major power plants, and 450,000 miles of high voltage transmission lines and numerous standards and regulations (American Public Power Association 2015; Executive Office of the President 2013). In Hughes' (1983) foundational history, the grid is a paradigmatic sociotechnical system; the social and technological aspects of the system were engineered together, such that changes in the political and regulatory environment may necessitate technological changes, and vice versa. In recent decades, changing regulations and associated technologies have increased complexity (Hirsh 1999; Latham 2004; Perrow 2007; Rinaldi et al. 2001). Practitioners are keenly aware of this; as one stated, 'Complexity is increasing every day'. This increasing complexity increases the chances of 'normal accidents' (Perrow 1984) and other types of disasters. As another utility employee said 'Murphy regularly finds its way into the utility business. Things like perfect storms happen all the time'.

### 3.1 Incentives

> 'You look at the industry prior to the standards and it's night and day'
>
> —former utility employee and auditor

The incentives created by the NERC CIP standards were shaped not only by the codified standards themselves, but by the ways that top-level leaders in organisations interpreted the wording of the standards. This is because utilities are hierarchical, with technical cybersecurity staff often insulated from key decision makers. A former utility employee stated that technical staff were typically 'like, three steps below even a senior manager' and that 'it would be a career-limiting move to go straight to the CEO'. Because the executive level is 'where resources are allocated', one executive noted the importance of leadership for ensuring cybersecurity.

Most leaders responded to the CIP standards by allocating additional resources to security. The CEO of a large utility explained that at the executive level 'all issues were competing against each other' for limited resources. Leaders with cybersecurity backgrounds tended to

consider cybersecurity to be more important and devote more resources to it than did those without cybersecurity backgrounds. However, few leaders have cybersecurity backgrounds. Instead, they have backgrounds in areas such as law, electrical engineering, and business management. Thus, a former utility employee and regulator stated that company executives 'are still not getting the cybersecurity aspect of this. They are being driven primarily by the risk of violation penalties'. Another stated: 'the reality is, cybersecurity has never been seen as a core part of the business. And it's still not'.

While leaders consider reliability to be important, cybersecurity has not been an issue of great concern. Cybersecurity is a cost centre, not a profit maker. Reputational risks associated with violating regulations were cited as having greater impact than associated fines. An auditor and former utility employee stated that executives 'don't want to be on Capitol Hill or in the newspapers' or face other types of negative publicity associated with violations. Negative publicity affected profit: it could reduce investor confidence and lead to questions from public utility commissioners who set rates and impose regulations at the state level.

Although organisational leadership and the resulting budget priorities influenced how cybersecurity risks were addressed, organisations changed their structure and allocated more resources to cybersecurity in response to the standards. Information technology (IT) staff working for organisations without strong cybersecurity leadership described standards as useful for protecting their budgets in the face of resource constraints; one believed that without standards, cybersecurity budgets would be cut because their organisation did not take cybersecurity seriously. The specific requirements of the standards could also serve as a tool for communicating cybersecurity resource needs. Instead of engaging leadership in esoteric technical discussions, IT staff could simply list what they needed to comply with the standards. The standards also brought new awareness of cybersecurity risk to the executive level, and in some cases increased executive-level cybersecurity expertise as executives hired additional leaders with cybersecurity expertise.

At the operational level, the standards forced cybersecurity into what was previously the domain of the sector's main tacticians, electrical engineers. For instance, patching requirements were a 'huge blessing' because they demanded that reviews be performed regularly instead of 'weeks or months or whenever you can get to it', said one IT expert. Because of the standards, engineers who mainly viewed cybersecurity as conflicting with reliability requirements now had to engage with cybersecurity.

Organisations often made dramatic changes in their security practices to comply with the standards. Among other activities, compliance required segmenting networks, performing employee background checks and trainings, and installing fences and other physical security perimeters. Enacting these requirements improved the security posture of many organisations; a former employee of a large investor owned utility described their organisation's cybersecurity measures before the standards as '[a]lmost non-existent', adding: 'Control systems were not segregated. Networks were just flat'. With the standards, his organisation was 'starting to get an inkling' of the importance of security. Organisations also increased the resources being devoted to cybersecurity: one company tripled the number of IT staff supporting control centres and another quadrupled its staff.

While the standards created an incentive for compliance, their impact on security was shaped not only by leadership, but by the prior state of utilities' cybersecurity programmes. Smaller utilities had fewer resources to spend on cybersecurity than larger ones and thus did not often have robust cybersecurity programmes. They often used the standards as a security guide, helping to establish a common baseline or threshold for security in the industry. However, larger organisations often had to modify pre-existing cybersecurity programmes to fit with regulatory requirements, sometimes in ways that reduced security. For instance, one utility with a policy of monthly cybersecurity scans—well beyond the yearly scanning requirements of the CIP standards—received a non-compliance violation after it failed to scan during a month when it was responding to severe storms. Since policies that differed from the standards increased compliance risk, utilities modified their cybersecurity policies to match CIP specifications—and sometimes this meant reducing their cybersecurity requirements.

As this suggests, the auditors who evaluated compliance documentation also shaped the incentives created by the standards. One utility employee likened them to an 'umpire' in a game of baseball, interpreting the formal rules to fit specific and unique contexts. Merely preparing for an audit was a time-consuming task that at times could distract from security. Compliance paperwork could consist of thousands of pieces of evidence that did little to improve security. 'A much greater portion of every dollar is spent on CIP [compliance] than on cybersecurity', stated a consultant involved in CIP compliance, a comment confirmed by many respondents. Extensive documentation was necessary to ensure requirements were being followed and to reduce reputational risk—which remained the primary concern among most leaders and drove resource allocation. The overall effort to comply and demonstrate compliance did not always match perceived security benefits. The standards 'require certain things, and sometimes it creates a lot of work that doesn't provide a lot of security value' said a former auditor and IT expert.

In sum, the incentives created by the standards were a result of interactions between written regulations, organisational leadership, and auditing practices. While these complex interactions were deliberately intended by those who designed the regulatory process, some of the resulting incentives were not. Specifically, the resulting incentives helped to create both a 'floor' for utilities with initially low cybersecurity standards, and a 'ceiling' for utilities that already had strong programmes in place. One regulator characterised the standards as 'kind of push[ing] from both the bottom and the top to the middle', moving an industry towards a common level of cybersecurity.

### 3.2 Scope

> 'It's like the Maginot Line'
>
> —employee of a non-profit focused on infrastructure

The Maginot Line is a line of fortifications that the French government constructed on its German borders in the 1930s to protect against invasion. It was a formidable defence, but during World War II, Germans bypassed the line by entering France via Belgium. Like the Maginot Line, the CIP standards offer a strong defence, but can be circumnavigated due to the high interconnectivity between what is regulated—the BES—and relatively unregulated systems, such as fuel supplies, distribution, and communications.

As noted previously, the CIP standards are limited jurisdictionally to the BES, which includes electric generation and transmission but not distribution. A former regulator described distribution as 'still mostly asleep at the wheel' and a consultant stated that if he wanted to compromise the electric system, he 'would go through the distribution system, because that's currently unregulated' rather than attack the BES. Compromising a distribution system could leave a 'whole city without power', said a former utility employee. To illustrate the

dangers that distribution posed, a former regulator and utility employee noted that the 2003 Northeast blackout was initially triggered by distribution assets, calling this a 'litmus test'. Others cited the 2015 cyberattacks on Ukraine's electricity distribution systems, which left approximately 200,000 people without power.

Other infrastructures were identified as crucial but also outside the jurisdiction of the CIP standards: '[t]he gas system isn't NERC CIP compliant, and the supply chain isn't NERC CIP compliant, and the transportation systems that carry coal on trains or on barges to the power plants… none of that is NERC jurisdictional either.' Somewhat artificial lines between the BES and these other systems were determined during the standards development process. A regulator described how communications infrastructure, where false information could potentially be injected into control centres, was ruled as out of scope 'because the industry—the utilities—don't own those wires, the phone company does'. These boundaries sharply limited the scope of the standards: an auditor stated that they could 'ask up to the point of where the fuel enters—whether it's coal or gas or anything—but after that it's out of scope'.

Organisations attempted to escape compliance burdens by reducing the number of their assets which fell under the scope of the standards. These activities could strengthen security: segmenting critical from non-critical systems removed non-critical systems from CIP jurisdiction and also reduced the attack surface and interactive complexity of critical assets. They could also reduce security. For example, the first version of the standards classified black start devices, generation that can start without support from the electric grid, as 'critical' and subject to regulations. As many as 25 percent of organisations chose to remove black start devices rather than maintain compliance, reducing the grid's resilience (NERC 2015). Likewise, serial communications were not subject to security requirements but routable protocols were; to reduce compliance some organisations replaced routable protocols with insecure serial protocols, even though routable protocols could be made more secure (Ladendorff 2014). One utility employee commented on dangerous strategies he had seen used to limit compliance burden: 'My favourite one is the tag on the cable that says "unplug this cable before audit"'.

A few contended that efforts to minimise scope also occurred when developing standards: 'what they [utilities] want to do is push minimalist requirements as high up into that stack as they can so that they're not doing all this super-rigorous stuff', said a regulator, arguing that industry-led standard development processes facilitated regulatory capture and resulted in minimalist regulations.

By contrast, some organisations effectively expanded the scope of the standards. For example, some utilities found it more efficient to have the same cybersecurity protection regime for all assets, so they managed assets outside the standards' official scope to CIP specifications. The standards were a 'forcing function' for considering security across an organisation, said one former utility employee: 'You can't manage one part of your company to the NERC level and ignore the business side.' However, not all organisations chose to enlarge the scope of the standards. One consultant who inquired into why a utility had weak distribution-level cybersecurity received the response: 'well, every time we try to [implement cybersecurity in distribution] the answer we get from the business is there's no regulatory requirement that makes us do that'.

### 3.3 Adaptability

> 'You look at CIP v1 right now and you compare it to CIP v5 – they're not even the same universe. CIP v5 is so much better'
>
> —former regulator

> 'There is a dynamic nature to cyber threat that has a lot of change, that goes fast. Standards are not fast'
>
> —former regulator

The CIP standards are designed to be modified as the sector changes, and have a certain level of adaptability. For instance, a former utility employee described the early wording and terminology of the standards as 'a legal nightmare' that led to conflicts between utilities and auditors; others pointed to early flaws that allowed compliance to supersede security and that limited scope. The standards were modified in response to these shortfalls, for example, by removing distinctions between routable and serial protocol types, by establishing standardised risk assessment criteria, by developing physical security standards, and by adopting less combative audit approaches. These changes have improved the regulations by aligning them with the risk and institutional profiles of the sector (Ellis 2014).

However, developing new standards was and remains a slow process; revising an existing reliability standard takes about twenty-seven months, and creating a new standard around forty months (NERC 2014). Stakeholders argue that it would be dangerous to speed up standards development because it must be a consensus-driven process that includes complex interactions between many actors. As noted previously, new standards need approval from FERC and NERC in addition to a broad supermajority vote of approval from utilities. Since utilities have different pieces of technology, different organisational structures, and different roles in the electric system, they also have different views on how the standards should be structured. Conflict was particularly prevalent during the initial standard drafting process: 'We fought and we fought and fought. And then we would go have drinks and laugh and come back the next day and fight all over again', said a member of the initial drafting team.

Although most standards development involves conflict and drinking, the CIP standards were particularly difficult to develop because the expertise needed for the standards was so nascent, as it required bridging the gap between operational technology and IT (Slayton and Clark-Ginsberg 2018). Operational technology included supervisory control and data acquisition (SCADA) systems—computers used to control physical machinery—in which frequent updates and other security practices were frowned upon because they could create risks to reliability. Drafting teams could not use other standards as models since few other operational technology infrastructures had cybersecurity regulations in place. 'We invented terms; we're just like, well, what is that?' said a member involved in the standard development process. Words needed to be defined to suit the sociotechnical environment of the BES; developing definitions could take days due to the complexity of this environment. Notably, the amount of time required for drafting the cybersecurity standards was significantly longer than for more traditional reliability standards, precisely because of the novelty of the problem (Slayton and Clark-Ginsberg 2018).

Some argue that the standards will be rapidly outdated because of changing technology. A former drafting team member stated that the CIP standards were 'no magic solution' to the common problem of regulations not fitting with new technologies. 'Technology changes at a much faster pace than the standards language', said a regulator. As a result, '[t]he laws lag behind the technology by years.' Because the standard did not discuss these new technologies, utilities were wary of investing in them, since they would have to reconfigure systems if standards were subsequently developed. A control system researcher felt that the standards 'stifle innovation.

A lot of innovative things that could have happened [do] not because of threat of standards and violation of standards'.

However, some engineers argue that the industry's embrace of new technologies has created security vulnerabilities; from this perspective, regulations slowing the embrace of new technology may be desirable. A group of cybersecurity professionals in the energy industry recently attempted to counter 'our infatuation with technology and technological fixes' by highlighting the vulnerabilities that grow with increasing technological complexity (Assante et al. 2015). Similarly, many engineers have expressed caution about new technologies such as the cloud. As one wrote on a mailing list concerned with SCADA security, 'the cloud provider has security risks, but overall they are fewer than if the entity hosted the information itself because the cloud provider is more competent/efficient at doing security' (Whitsitt 2016). Another engineer replied that 'this leaves out the risk introduced by creating a more complex overall picture' (Highfill 2016). Yet another engineer acknowledged these risks but continued: 'there are many small scale SCADA users who cannot and should not attempt to manage the security of their SCADA system. They can barely spell SCADA correctly' (Brodsky 2016).

Such disagreements and ambiguities about exactly which organisations would benefit from new technologies such as the cloud are a major reason that the standards do not discuss them. While potentially inhibiting certain innovations in areas that could improve grid efficiency and reliability, the standards spurred innovation in security-focused technologies. The CIP standards spawned a broader industry focused on supporting utilities implementing the standards. Many vendors emerged to develop specific products to facilitate compliance, such as fences and other devices for physical security and software for tracking compliance. This market ballooned, and today numerous companies offer wide-ranging products and services, many tailored to the specific and cybersecurity and compliance needs of the electric sector. Organisations such as EnergySec, a non-profit focused on electric grid security and compliance, and SANS, a for-profit cybersecurity training organisation, developed courses and began to train utility employees and regulators on compliance. NERC and regional entities also developed 'best practices' to help utilities implement the standards in a manner that minimised negative compliance repercussions. The standards thus facilitated the development of expertise and a broader industry that could help the industry adapt to its changing environment (Slayton and Clark-Ginsberg 2018).

Adapting the standards to a changing environment, however, could create problems. A former regulator explained that any change that 'circumvents the controls' imposed by previous standards could prevent utilities from recovering their investments. A former utility employee objected that continually changing the standards would 'drive utilities completely insane' since it forced utilities to make security and compliance reconfigurations that could be financially costly. The standards' adaptability requires good communication between utilities, auditors, standards drafting teams, and the regulatory organisations, FERC and NERC. Fear of violations initially discouraged regulated organisations from talking with regulators. 'We're all so afraid to talk to each other, and everybody's so afraid of this regulatory environment and these fines' said a former regulator. Some utility employees hesitated to ask regulators questions because they feared questions would lead to additional scrutiny during audits. While some early audits were heavy-handed and created tensions between auditors and utilities, communication improved as regulators shifted towards less combative forms of auditing.

## 4. Discussion and conclusion

As this analysis shows, regulatory incentives, scope, and adaptability can only be understood as an emergent product of interactions between formal regulations and the larger sociotechnical system of which they are a part. This conception helps to clarify the powers and limitations that regulations have in affecting change.

Proponents and detractors of the CIP standards described how the standards both directly influenced cybersecurity practices and indirectly reshaped utility operations and management. While establishing a threshold of security at each individual organisation is crucial, we suggest that the more profound influence of the standards lies in the ways that they interacted with and altered the complex sociotechnical system that is the electric power grid. Organisations restructured some of their key operations, bringing in lawyers and administrators to address areas previously dominated by engineers and creating new divisions to reduce their compliance risk. The standards drafting process fuelled the development of both a new area of expertise and a new industry that could bridge the gap between operational technology and information security. Furthermore, the risk of regulatory capture by the utility industry was somewhat mitigated by the information security industry's interest in tough standards (Slayton and Clark-Ginsberg 2018).

However, not all emergent changes to the sociotechnical system enhanced security. An excessive focus on compliance could distract from cybersecurity and hinder information sharing, and some organisations even reduced their security standards to avoid being penalised for non-compliance. While many system level changes emerged from the standards, changes arose out of individual responses to regulations that were dependent on the unique *local* configuration of the sociotechnical system. The size, composition, and interactions of generating facilities, transmission lines, computing and networking technologies, regulated organisations, manufacturers, professional groups, and regulators varied across territories and meant that local responses to standards were unique. Thus, the locally-influenced actions of individual actors combined to create emergent system-level outcomes, which in turn shaped the actions of individual actors.

Understanding regulations as part of an emergent sociotechnical system has important implications for the process of regulatory design. It points to the need to consider not only immediate effects of regulations but also the ways in which auditors and regulated entities participate in shaping the effective incentives, scope, and adaptability of standards. Although the potential for unintended consequences is well-recognised in scholarship on regulation, there is relatively little advice on how to avoid such consequences, and the history of NERC CIP suggests that regulators may still be failing to anticipate and prevent the creation of perverse incentives. For example, it is not surprising that utilities would respond to the imposition of expensive security requirements on black start equipment by simply shedding them, particularly since such equipment is not central to daily operation. One way to better anticipate such consequences is for regulators to more explicitly consider the active role of regulated entities, auditors, and other key actors in shaping the incentives, scope, and adaptability of formal rules, focusing on the individual decisions of those actors in response to policy changes and how those responses might interact to shape the electric grid as a system.

While a focus on the active role of regulated entities, auditors, industry organisations, and other actors in the system could improve regulatory outcomes, the complex and emergent nature of sociotechnical systems means that system level outcomes will never be completely predictable. As this case illustrates, steering the development

of complex systems through regulation is challenging because the effects of the regulations are ultimately products of the emergent interactions between written laws and complex and locally specific sociotechnical systems. Even the most carefully designed sets of regulations will likely result in unforeseen positive and negative outcomes due to the complexity of the electric power system. This impossibility of completely predicting how regulations influence complex systems points to the need to seek out, identify, and react to the unexpected interactions with regulations as they emerge, and to design regulations in ways that keep failures localised rather than allowing them to compromise the entire system. In other words, instead of attempting to create infallible regulations, efforts should focus on creating resilient regulations, regulations that maintain their core functions despite the unexpected. The CIP standards already demonstrate many elements of regulatory resilience—they are updated regularly in response to emerging changes and they help disparate groups share information and learn from each other—but they also contain frictions that hinder resilience. As this analysis demonstrates, focusing on the key elements of regulatory influence, scope, and adaptability can improve the ability of the standards to interact as part of a complex sociotechnical system and ultimately improve regulatory resilience.

## References


Abraham, J., and Sheppard, J. (1999) 'Complacent and Conflicting Scientific Expertise in British and American Drug Regulation: Clinical Risk Assessment of Triazolam', *Social Studies of Science*, 29/6: 803–43.

American Public Power Association (2015) 'U.S. Electric Utility Industry Statistics'.

Ansell, C., Boin, A., and Keller, A. (2010) 'Managing Transboundary Crises: Identifying the Building Blocks of an Effective Response System', *Journal of Contingencies and Crisis Management*, 18/4: 195–207.

Assante, M., Roxey, T., and Bochman, A. (2015) 'The Case for Simplicity in Energy Infrastructure', <https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151030_Assante_SimplicityEnergyInfrastructure_Web.pdf> accessed 25 Oct 2017.

Ayres, I. and Braithwaite, J. (1992), *Responsive Regulation: Transcending the Deregulation Debate*. Oxford: Oxford University Press.

Bijker, W. E., Hughes, T. P., and Pinch, T. J. (eds) (1987) *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*. Cambridge, MA: MIT Press.

Boin, A. (2009a) 'Meeting the Challenges of Transboundary Crises: Building Blocks for Institutional Design', *Journal of Contingencies and Crisis Management*, 17/4: 203–5.

—— (2009b) 'The New World of Crises and Crisis Management: Implications for Policymaking and Research', *Review of Policy Research*, 26/4: 367–77.

Bowker, G. C., and Star, S. L. (2000) *Sorting Things Out: Classification and Its Consequences*. Cambridge, MA: The MIT Press.

Braithwaite, J. (1982) 'Enforced Self-Regulation: A New Strategy for Corporate Crime Control', *Michigan Law Review*, 80/7: 1466–507.

Brodsky, J. (2016) 'Progress or Impending Doom?', *SCADASEC Digest*, 99/44. <http://scadasec.email/pipermail/scadasec/2016-April/028981.html> accessed 16 Oct 2018.

Busch, L. (2011) *Standards: Recipes for Reality.* Cambridge, MA and London: MIT Press.

Centeno, M. A., Nag, M., Patterson, T. S. et al. (2015) 'The Emergence of Global Systemic Risk', *Annual Review of Sociology*, 41: 65–85.

Clark-Ginsberg, A., Abolhassani, L., and Rahmati, E. A. (2018) 'Comparing Networked and Linear Risk Assessments: From Theory to Evidence', *International Journal of Disaster Risk Reduction*, 30: 216–224.

Coglianese, C., and Mendelson, E. (2010) 'Meta-Regulation and Self-Regulation', in M. Cave, R. Baldwin, and M. Lodge (eds) *The Oxford Handbook of Regulation*, pp. 146–68. New York: Oxford University Press.

——Nash, J., and Olmstead, T. (2003) 'Performance-Based Regulation: Prospects and Limitations in Health, Safety, and Environmental Protection', *Administrative Law Review*, 55/4: 705–29.

Demeritt, D., Rothstein H. and Beaussier A. -L. et al. (2015) 'Mobilizing Risk: Explaining Policy Transfer in Food and Occupational Safety Regulation in the UK', *Environment and Planning A*, 47/2: 373–91.

Department of Homeland Security (2015), 'NCCIC/ICS-CERT Year in Review', (National Cybersecurity and Communications Integration Center/Industrial Control Systems Cyber Emergency Response Team).

Downer, J. (2010) 'Trust and Technology: The Social Foundations of Aviation Regulation', *The British Journal of Sociology*, 61/1: 83–106.

Eisner, M. A. (2017) Regulatory Politics in an Age of Polarization and Drift: Beyond Deregulation. New York, NY: Taylor & Francis.

Ellis, R. (2014) 'Regulating Cybersecurity: Institutional Learning or a Lesson in Futility?', *IEEE Security & Privacy*, 12/6: 48–54.

FERC (2008) *Mandatory Reliability Standards for Critical Infrastructure Protection' Docket No. RM06-22-000; Order No. 706*, 99/44. <https://www.ferc.gov/whats-new/comm-meet/2008/011708/E-2.pdf> accessed 16 Oct 2018.

Executive Office of the President (2013), 'Economic Benefits of Increasing Electric Grid Resilience to Weather Outages', (The White House).

Gilad, S. (2010) 'It Runs in the Family: Meta-Regulation and Its Siblings', *Regulation & Governance*, 4/4: 485–506.

Gormley, W. T. (1986) 'Regulatory Issue Networks in a Federal System', *Polity*, 18/4: 595–620.

Grabosky, P. N. (1995) 'Counterproductive Regulation', *International Journal of the Sociology of Law*, 23: 347–69.

Haines, F. (2011) 'Addressing the Risk, Reading the Landscape: The Role of Agency in Regulation', *Regulation & Governance*, 5/1: 118–44.

Hart, D. (2007) 'Understanding Immigration in a National Systems of Innovation Framework', *Science and Public Policy*, 34/1: 45–53.

Hecht, G. (1998) *The Radiance of France: Nuclear Power and National Identity after World War II*. Cambridge, MA: MIT Press.

—— (2001) 'Technology, Politics, and National Identity in France', in M. T. Allen and G. Hecht (eds) *Technologies of Power: Essays in Honor of Thomas Parke Hughes and Agatha Chipley Hughes*, pp. 253–93. Cambridge, MA, and London: MIT Press.

Highfill, D. (2016) 'Progress or Impending Doom?', *SCADASEC Digest*, 99/44. <http://scadasec.email/pipermail/scadasec/2016-April/028979.html> accessed 16 Oct 2018.

Himmelsbach, R. (2017) 'How Scientists Advising the European Commission on Research Priorities View Climate Engineering Proposals', *Science and Public Policy*, 45/1: 124–133.

Hirsh, R. F. (1999) *Power Loss: The Origins of Deregulation and Restructuring in the American Electric Utility System*. Cambridge, MA: MIT Press.

Hood, C., Rothstein, H. and Baldwin, R. (2001) *The Government of Risk: Understanding Risk Regulation Regimes*. Oxford: Oxford University Press.

Huber, P. W. (1985) 'The Bhopalization of U.S. Tort Law', *Issues in Science and Technology*, 2/1: 73–82.

Hughes, T. (1983) *Networks of Power: Electrification in Western Society, 1880–1930*. Baltimore, MD: Johns Hopkins University Press.

Hughes, T. P. (1987) 'The Evolution of Large Technological Systems', in W. E. Bijker, T. P. Hughes, and T. J. Pinch (eds) *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*, pp. 51–82. Cambridge, MA: MIT Press.

Jasanoff, S. (1990) *The Fifth Branch: Science Advisors as Policymakers*. Cambridge, MA: Harvard University Press.

—— (2005). *Designs on Nature*. Princeton, NJ: Princeton University Press.

Ladendorff, M. Z. (2014) *The Effect of North American Electric Reliability Corporation Critical Infrastructure Protection Standards on Bulk Electric System Reliability*, Capella University.

Lampland, M. and Star, S. L. (2009) *Standards and Their Stories: How Quantifying, Classifying, and Formalizing Practices Shape Everyday Life*. Cornell: Cornell University Press.

Latham, R. (2004) *Bombs and Bandwidth: The Emerging Relationship between Information Technology and Security*. New Delhi: Manas Publications.

Le Coze, J-c. (2005) 'Are Organisations too Complex to Be Integrated in Technical Risk Assessment and Current Safety Auditing?', *Safety Science*, 43/8: 613–38.

Macrae, C. (2010) 'Regulating Resilience? Regulatory Work in High-Risk Arenas', in B. Hutter (ed.) *Anticipating Risks and Organizing Risk Regulation*, pp. 139–60. Cambridge: Cambridge University Press.

Manyena, S. B. (2006) 'The Concept of Resilience Revisited', *Disasters*, 30/4: 434–50.

May, P. J. (2007) 'Regulatory Regimes and Accountability', *Regulation & Governance*, 1/1: 8–26.

McGoey, L. (2007) 'On the Will to Ignorance in Bureaucracy', *Economy and Society*, 36/2: 212–35.

McLean, C. and Patterson, A. (2012) 'The Regulation of Risk: Mobile Phones and the Siting of Phone Masts – The UK Experience', *Science and Public Policy*, 39/6: 827–36.

NERC (2014) 'Analysis of NERC Standards Process Results Fourth Quarter 2013', (North American Electric Reliability Corporation).

—— (2015) 'CIP-002–5.1a—Cyber Security—BES Cyber System Categorization' (North American Electric Reliability Corporation).

O'Neil, P. D. (2011) 'High Reliability Systems and the Provision of a Critical Transportation Service', *Journal of Contingencies and Crisis Management*, 19/3: 158–68.

——Krane, D. (2012) 'Policy and Organizational Change in the Federal Aviation Administration: The Ontogenesis of a High-Reliability Organization', *Public Administration Review*, 72/1: 98–111.

Padgett, J. and Powell, W. (eds) (2012) *The Emergence of Organizations and Markets*. Princeton, NJ: Princeton University Press.

Perrow, C. (1984) *Normal Accidents: Living with High-Risk Technologies*. Princeton, NJ: Princeton University Press.

Perrow, C. (2007) *The Next Catastrophe: Reducing Our Vulnerabilities to Natural, Industrial, and Terrorist Disasters*. Princeton, NJ: Princeton University Press.

Perrow, C. (2015) 'Cracks in the "Regulatory State"', *Social Currents*, 2/3: 203–12.

Pescaroli, G. and Alexander, D. (2015) 'A Definition of Cascading Disasters and Cascading Effects: Going Beyond the "Toppling Dominos" Metaphor', *Planet@ Risk*, 3/1: 58–67.

Pettersen, K. A. and Bjørnskau, T. (2015) 'Organizational Contradictions between Safety and Security–Perceived Challenges and Ways of Integrating Critical Infrastructure Protection in Civil Aviation', *Safety Science*, 71: 167–77.

Rees, J. V. (1988) *Reforming the Workplace: A Study of Self-Regulation in Occupational Safety*. Philadelphia, PA: University of Pennsylvania Press.

Rinaldi, S. M., Peerenboom, J. P., and Kelly, T. K. (2001) 'Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies', *Control Systems, IEEE*, 21/6: 11–25.

Sagan, S. (1993) *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons*. Princeton, NJ: Princeton University Press.

Schulman, P., and Roe, E. (2016) *Reliability and Risk: The Challenge of Managing Interconnected Infrastructures*. Stanford, CA: Stanford University Press.

Sen, A. (2014) 'Totally Radical: From Transformative Research to Transformative Innovation', *Science and Public Policy*, 41/3: 344–58.

Shohet, S. (1996) 'Biotechnology in Europe: Contentions in the Risk-Regulation Debate', *Science and Public Policy*, 23/2: 117–22.

Shreve, C. M., and Kelman, I. (2014) 'Does Mitigation Save? Reviewing Cost-Benefit Analyses of Disaster Risk Reduction', *International Journal of Disaster Risk Reduction*, 10: 213–35.

Silbey, S. S. (2009) 'Taming Prometheus: Talk about Safety and Culture', *Annual Review of Sociology*, 35: 341–69.

Slayton, R. and Clark-Ginsberg, A. (2018) 'Beyond Regulatory Capture: Coproducing Expertise for Critical Infrastructure Protection', *Regulation & Governance*, 12/1: 115–30.

Star, S. L. (1999) 'The Ethnography of Infrastructure', *American Behavioral Scientist*, 43/3: 377–91.

——Ruhleder, K. (1996) 'Towards an Ecology of Infrastructure', *Information Systems Research*, 7/1: 111–34.

——Lampland, M. (2009), 'Reckoning with Standards', in S. L. Star and M., Lampland (eds), *Standards and Their Stories: How Quantifying, Classifying, and Formalizing Practices Shape Everyday Life*. Ithaca, NY: Cornell University Press.

Sunstein, C. (1990) 'Paradoxes of the Regulatory State', *University of Chicago Law Review*, 57: 407–41.

Taleb, N. N. and Blyth, M. (2011) 'The Black Swan of Cairo: How Suppressing Volatility Makes the World Less Predictable and More Dangerous', *Foreign Affairs*, 90/3: 33–9.

Turner, B. A. and Pidgeon, N. F. (1997) *Man-Made Disasters (2: JSTOR)*. Oxford: Butterworth-Heinemann.

U.S.-Canada Power System Outage Task Force (2004) 'Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations'.

Vaughan, D. (1989) 'Regulating Risk: Implications of the Challenger Accident', *Law & Policy*, 11/3: 330–49.

—— (1999) 'The Dark Side of Organizations: Mistake, Misconduct, and Disaster', *Annual Review of Sociology*, 25: 271–305.

Weick, K. E. and Sutcliffe, K. M. (2011) *Managing the Unexpected: Resilient Performance in an Age of Uncertainty*. San Francisco, CA: John Wiley & Sons.

Wetmore, J. M. (2004) 'Redefining Risks and Redistributing Responsibilities: Building Networks to Increase Automobile Safety', *Science, Technology, & Human Values*, 29/3: 377–405.

Whitsitt, J. (2016) 'Progress or Impending Doom?', *SCADASEC Digest*, 99/44. <http://scadasec.email/pipermail/scadasec/2016-April/028978.html> accessed 16 Oct 2018.

Wildavsky, A. B. (1988) *Searching for Safety*, Vol. 10. New Brunswick: Transaction Publishers.