

Reinventing the Relationship Between Operators and Regulators

Editor: David Costello, *Schweitzer Engineering Laboratories, Inc.*

Abstract—The sharing of information, such as the root cause of misoperations and the lessons learned from those events, has long been a valuable part of the overall efforts of the power industry to improve the reliability of electric power. However, the fear of audits, noncompliance fines, competitive disadvantage, and lawsuits has injured our ability to discuss, teach, and learn. We share a responsibility to work together to improve power system reliability.

At the Modern Solutions Power Systems Conference in June 2014 in Houston, Texas, a panel discussed these topics in a four-hour session. The panel consisted of Kristian Koellner, supervisor of system protection at the Lower Colorado River Authority; Michael Moon, senior director of regional entity coordination at the North American Electric Reliability Corporation; Mark Henry, director of reliability at Texas Reliability Entity, Inc.; Martin Golden, partner and attorney at Keogh, Cox, & Wilson, Ltd. (a professional law corporation); Christopher Hart, acting chair of the National Transportation Safety Board; and David Costello, the technical support director at Schweitzer Engineering Laboratories, Inc. This paper is an edited transcript of the audio and video recordings of the presentations and discussions from that session.

The discussion addresses the following questions and concerns. Are present regulations and compliance efforts improving reliability? What best practices of other industries can we follow? What can be done to balance required mandatory and enforceable standards with the sharing of information? How can our industry move toward an environment where safe harbor is provided to good people who are trying to do the right thing?

I. INTRODUCTION

David Costello,

Schweitzer Engineering Laboratories, Inc. (SEL)

Engineers investigate, learn, share information and what we know, teach, and work together to solve problems and improve the power system. But the Northeast blackout in 2003 brought sweeping legislative and regulatory changes, including mandatory and enforceable standards. Misoperations and power outages can result in lawsuits. Our environment shapes our behavior, and this is not always a good thing. My premise for assembling this panel was simple. I believe that the fear of audits, compliance fines, competitive disadvantage, and lawsuits has injured our ability to work together and share information. We are a little less likely to share because we are fearful of the risks and consequences that we bring upon ourselves and our organizations. I did not have any grandiose or naive assumptions that we were going to solve all of the industry's problems in an afternoon, but I hoped that the assembled group of experts would influence the discussion and move it in the right direction. We need to improve, and I think there are good people working hard to do just that.

In reading this transcript, you will learn from a utility—a registered entity in our bulk electric system (BES)—and understand better their perspective on the impact of regulation, the challenge of sharing, and results to date. From regulators, both at the North American Electric Reliability Corporation (NERC) and Texas Reliability Entity, Inc. (Texas RE), you will read a historical perspective on industry regulation and learn about the current efforts to move away from check-the-box compliance and fines to a focus on reducing risks and improving reliability. An attorney reminds us that our good intentions must be balanced by a legal reality check and that our industry needs safe harbor. Lastly, we endeavor to learn from the aviation industry's success. Aviation has been sharing information for many years in a confidential way that provides assurance that the reporter is not going to be fined or punished for sharing. The Commercial Aviation Safety Team (CAST), in particular, is a model for regulator, operator, and manufacturer collaboration that we should emulate.

I have done my best to edit the audio and video transcripts of our session into a document that is interesting to read and true to the original speakers' words and presentations. The sections are presented in the order of the speakers that day, and the question and answer session that followed is presented as this paper's discussion and conclusions. The glossary of terms defines the acronyms used throughout this paper by the panel members. I hope you will join us in the effort to improve our industry.

II. THE CHALLENGE OF SHARING:

TRYING TO DO RIGHT BY COMPLIANCE

Kristian "Kris" Koellner,

Lower Colorado River Authority (LCRA)

When asked to participate on this panel, I thought it sounded great, but I had trouble coming up with the title. I finally settled on "The Challenge of Sharing" because one of the themes is that we all want to do better and we all want to help our fellow industry person do better, but sometimes that is hard to do. It is hard to share, to give back, for many reasons—you may not have time, you may not have the inclination, you may not have the management support. I snuck in a subtitle, "Trying to Do Right by Compliance," because that is what all of this is about.

My perspective is that of an operator—a utility, myself, and LCRA Transmission Services in Austin—and about life as a NERC entity, specifically the TO (transmission owner), TOP (transmission operator), and TP (transmission planner) perspectives. I will talk about challenges in two dimensions—

complexity, the overwhelming amount of stuff that you have to consider, look at, and deal with, and *churn*, the turnover in standards and the pace at which they change. I will share a few pitfalls where we actually stumbled and became familiar with the self-reporting process. I will conclude with some ideas on how to improve.

LCRA Transmission Services owns transmission assets. We are located in Austin, Texas, and we cover a pretty broad footprint, a good portion of Texas, with quite a few line miles at 345, 138, and 69 kV. With that comes a lot of owner, operator, and planner responsibilities. What is a little unique about us are all of the line miles that we operate for our electric cooperative members. LCRA has 43 wholesale customers, and we operate the transmission system for several of those. That means we have operating requirements in some cases for assets that we do not even own. So it gets to be tricky to figure out whether something is a TO, TOP, or TP requirement. Is this something that the cooperative needs to certify? Or, is this something within LCRA's role to certify? This is something unique that we are faced with, and it amounts to lots of assets and exposure.

June 18, 2014, is the seventh anniversary for the mandatory standards. When things became mandatory, I was working for Salt River Project (SRP) in Phoenix in the Western Electricity Coordinating Council (WECC). Really, it just added another layer of enforcement. There is the Federal Energy Regulatory Commission (FERC), then NERC, and now that I am in Texas, there is the Electric Reliability Council of Texas (ERCOT), Texas RE, the Public Utility Commission of Texas (PUCT), and internal criteria and standards. It is like a seven-layer dip of enforcement, and you have to do right by all of them. It is a lot to get your arms around. In a different session this morning, there were concerns about people potentially spending more time on compliance than on the actual work itself, and that is legitimate. But this is the world that we live in.

So, with all those requirements, standards, criteria, there is no single individual or even a group that can be a subject matter expert (SME) on all the applicable standards. There is no one guru that handles all your NERC compliance issues and claims. Compliance becomes a part of doing business. It is not that different from other enterprise-wide requirements, such as safety, labor laws, and document retention. It becomes part of your daily cost of doing business, and like safety, it becomes embedded so much that it is second nature. If you integrate compliance into your work processes, if you embed it within the organization, then it should feel very natural.

We have a compliance group that consists of three staff members dedicated to company-wide compliance issues. From the variety of registrations that apply to LCRA, they shared the number of standards, requirements, and sub-requirements that we must manage (see Table I). You see some pretty big numbers when you get to the sub-requirements category. That may be the "R.1 bullet" on a particular standard, but there may be a lot that needs to happen to comply with it.

TABLE I
STANDARDS, REQUIREMENTS, AND SUB-REQUIREMENTS MANAGED BY LCRA

| Registration | Number of Standards | | Number of Requirements | Number of Sub-Requirements |
|--------------|---------------------|-----|------------------------|----------------------------|
| | Non-CIP | CIP | | |
| LCRA – TO | 8 | 18 | 162 | 237 |
| LCRA – TOP | 21 | 18 | 227 | 312 |
| LCRA – TP | 8 | – | 31 | 104 |

So that staff of three obviously does not deal with all of that directly. They essentially farm out the responsibility to different groups. We have ten responsible managers, and each of them is in charge of a suite of standards, a collection which naturally fall into his or her area. Beneath that a level, there are 22 SMEs. I am an SME, for example, for protection and control (PRC) standard PRC-023 on relay loadability and for facilities design, connections, and maintenance (FAC) standard FAC-001 about facility interconnection requirements, and more [1].

Essentially, we are "voluntold" to do these activities, and we just have to make room for it. This places many demands on staff that already has limited bandwidth. You have to fit this into your 40 or 50 hours per week, or whatever it is you end up working. I did a search for "NERC" in my inbox this weekend and came up with 1,010 items. There are a lot of comings and goings—standards, definitions, formal comments, ballot pools, drafting committees, and more. The definitions can be just as impactful as the standard. Formal comments are a part of the stakeholder process, as are informal comments. But what exactly is an *informal* comment? While it is great to have an impact on the whole process, being on a drafting committee is a huge commitment. On top of this, you still have your normal work to do. We have misoperation reporting requirements every quarter. We have reliability standard audit worksheets (RSAWs) to complete. We have to tuck away objective evidence so you can produce it when you need it during an audit. We have ongoing corrective action plans. There is just a lot to this, and the more you look, the more you find. Mike [Moon] and Mark [Henry] may have actual data on the number of components and requirements growing over time, but you have new opportunities all the time, and there is definitely an upward trend.

There is churn as well. Compliance is a moving target. You can be compliant on Monday and not compliant on Tuesday. That is a problem. You are never done with compliance, just like you are never done with education. There is no finish line because it is always moving. There are always new projects to look at and figure out. There are new standards subject to enforcement phasing in over time. There are revisions to existing standards—just when you think you have one under control, it comes up for revision. Consolidations and retirements are a nice thing, and maybe that can make things simpler, but it is still something to be aware of and manage. There are varying effective dates by requirement. You have to

read the fine print. New technology and concerns, such as geomagnetic disturbances (GMDs), electromagnetic pulses (EMPs), and Aurora, always come up. There is a lot of churning, and it is a complex environment.

People need and like electricity. Our industry did have a few blackouts before standards became mandatory. I was working in WECC in Phoenix when the 1996 blackouts occurred, and that was very impactful on our utility and all of WECC. Then in 2003, we had the blackout in the Northeast. As I tell my kids, you can take care of things yourself, or I am going to come take care of it for you. I kind of view the industry that way as well. We had some issues, and human nature is what it is. There will be good actors and bad actors in any industry, in any field. That is where standards can help bring everyone up to some minimum level. But things get complicated, especially in system protection.

Fig. 1 represents a small piece of the ERCOT system. I have been thinking a lot about this area because the Elroy

substation near Austin is serving the load for the X Games this June. We all remember the power outage during the Super Bowl in 2013. We really do not want to have a big outage when ESPN is broadcasting and guys are jumping. That would not be good for the event, Austin, or LCRA. So I have been thinking about this area a lot and just tallied it all up—15 BES breakers (all at 138 kV), two relays per breaker, and 100 settings per relay. The number of settings is a very conservative estimate, by the way, and I did not include things like display points or ancillary functions that are not critical. That gives 3,000 total relay settings in this small area. That is a lot to look at. A problem with any setting could lead to a PRC-004 reportable misoperation. That is life today. If a fault occurs, you want appropriate breakers to open and nothing else. When it works, it is great. When it does not, there is trouble. PRC-004 is just one example, too. PRC-023 may apply; PRC-005 may apply, so you have a lot of standards that are in effect. And, this is just a very small part of the system.

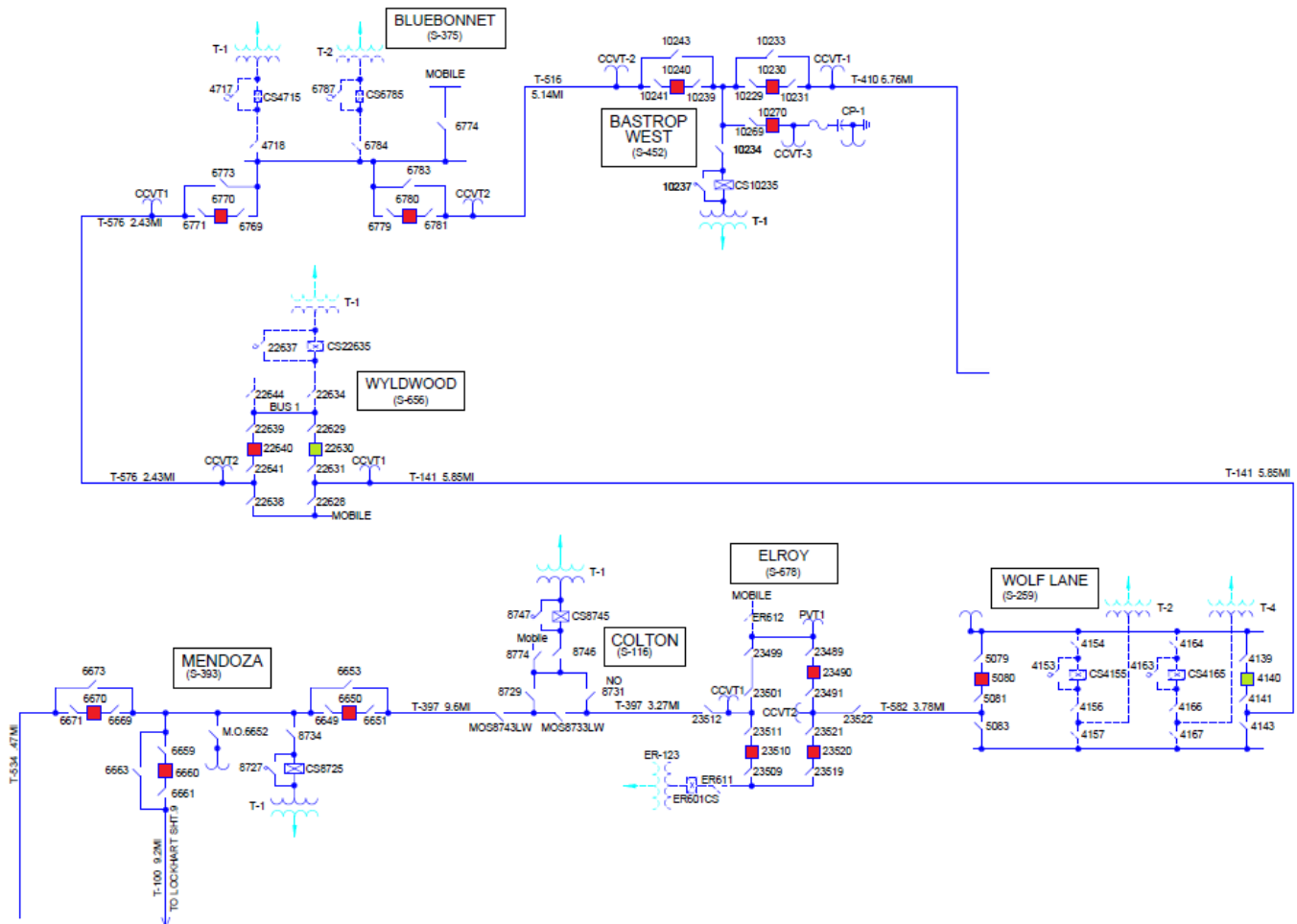


Fig. 1. Elroy Substation and a Small Piece of the ERCOT System

Fig. 2 shows how we are doing. This is the Texas RE relay misoperation trend over the last three years through the last quarter of 2013 [2]. Are we getting better? There is no improvement trend, but at least we are holding steady in the face of continued system growth, complexity, and more. There is definitely room for improvement.

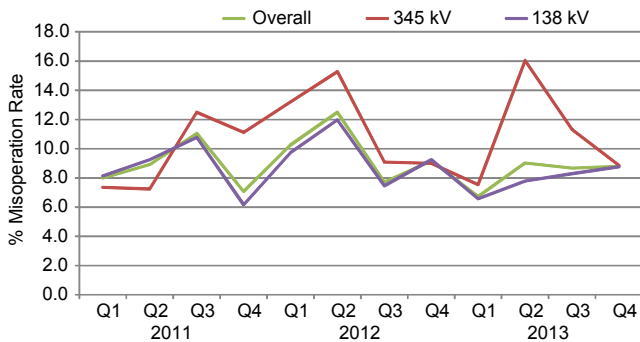


Fig. 2. Texas RE Region Misoperation Rate for the Last Three Years

Sometimes you drop the ball despite your best efforts. We had a PRC-023 transmission relay loadability violation that we chose to self-report. We energized two 345 kV, 3,278 A lines in February 2011. We discovered an error during an annual self-check of the settings in August 2011. Loadability was limited to a value above 100 percent of line rating, which is good, but to less than the required 150 percent of line rating dictated by PRC-023. So we had a problem with literally two out of the 100 or so settings mentioned before in two different relays, which led to a violation and a self-report. We worked with Mark Henry and his folks at Texas RE to go through the process. It was very interesting and, in the end, well received. I know that NERC and Texas RE and others encourage the self-reporting process, and I believe it is the right thing to do.

But, when you drop the ball, you have to be able to recover from that. We fixed the problem at that location and looked for the problem elsewhere. We tried to be very timely in doing all of this. We then shifted gears to discover where the mistake occurred in our process and how to prevent recurrence. We did not want to go through this pain again, and fortunately, we have not. It is a big focus for us. But something often left out of the discussion is how do you help others from having your same problem? How do we keep our neighbor from experiencing the same pain that we went through? And maybe they, in turn, can help us avoid some pain that they have incurred along the way.

There is a point in the self-reporting paperwork where you can list any mitigating factors, things that you have done to help the industry. At that point, it was very helpful, I believe, to be able to show what LCRA has done. We have done presentations at the Real World Experiences session at the Conference for Protective Relay Engineers at Texas A&M University, written and presented technical papers for industry conferences, led working groups at ERCOT, and we have tried to give back to the industry. I really feel that showed that we are trying our best to help others not have that same problem. In our case, I really think that helped to allow a \$0 penalty.

We had a violation, but because the ultimate fine was \$0, it was a success for us.

Besides that particular pitfall, Fig. 3 shows another noteworthy situation that we ran into. I mentioned that we serve 43 wholesale customers, and a lot of these customers own their own transmission systems. There are a lot of interconnections and tie points. You have all these different entities owning different components, and in this case, one of our customers was being audited. They caught some flack during the audit because they were asked for the maintenance records for their power transformer's high-voltage bushing current transformers (CTs). Those CTs are a part of our bus relay's zone of protection. We need a dependable and secure bus differential scheme, which is important for BES reliability. But because of this audit, there was concern over the power transformer CT ownership and its maintenance compliance implications. The step-down transformer, which is not part of the BES by itself, is owned by the customer. But, if that customer owns the high-voltage bushing CT that is tied into our bus differential scheme and that bus itself is part of the BES, what impact does that have on our customer? Does it now make them subject to PRC-005 because they own a piece of the protection system for that bus, simply because they own that CT in the power transformer bushing?

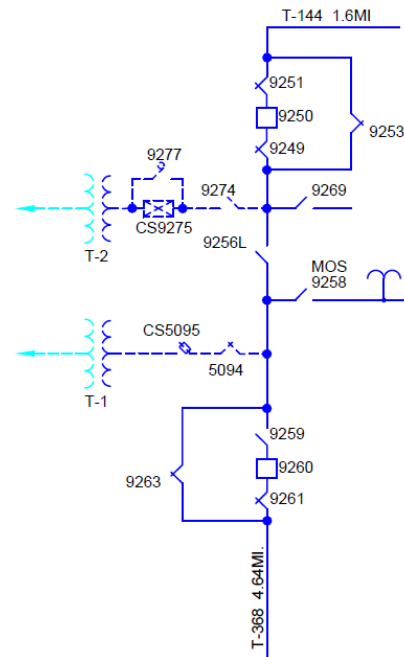


Fig. 3. A Case Study for PRC-005 and Unintended Consequences

The intention of the maintenance standard is good, but this exposed an unintended consequence. We brainstormed ways to fix this with the customer. We could turn the bus protection scheme into a partial differential, which would not be as fast, selective, or secure. We could add a standalone CT that would be owned by LCRA. This, however, is not cost-effective because we already have a perfectly good CT in that power transformer. Further, a standalone CT would add another

potential point of failure. All of this was only so that the customer can say, “We own this, and LCRA owns that, and we are out of the PRC-005 game. LCRA will own that responsibility.” We all understood the customer’s concerns, as they may not have any other transmission facilities and, from a corporate standpoint, do not want one CT dragging them into PRC-005 compliance requirements. But this case exposes issues where common sense and practicality sometimes lose out to check-the-box compliance.

The check-the-box syndrome is a real concern. Are you really designing the system to meet the needs of your customers, your situation, your region and the way it behaves? Or, are you just checking the box? Are you doing maintenance only when required? Are you designing schemes to just meet certain requirements? Are you just checking the box, or are you really thinking it through? Are we losing creativity? I know this also comes up in the planning arena. Although I am in system protection, I report up through the planning structure, so I sit and work with planners regularly, and we worry about that loss of creativity. If analysis shows that a line may overload and violate a transmission planning (TPL) standard, the easy answer may be to just upgrade the line. But maybe there is a more creative, cost-effective, and efficient solution. You need to look a little deeper. I wonder, how many violations out there are not self-reported because of the fear of penalty? How many presentations like this one are not happening because of the fear of penalty? What sharing and interaction is not going on because of the fear of penalty? What standards are being avoided, as in my bus differential example, because people are trying to steer clear of compliance situations and, in doing so, build a less reliable system? All of this is not good in the end. These are all pitfalls, and ultimately, we cannot see the forest for the trees. I worry that we may lose our whole purpose of trying to build a reliable and efficient system by just focusing on compliance, and it should not be that way.

So, given a complex, churning compliance environment (with the need to always do more with less) and a continent, literally, of utilities all facing common concerns, problems, worries, and issues, how do we prosper? Here are a few topics and tactics. First, it comes down to identifying a few vital priorities. If I have one hour to spend, where do you guys at NERC want me spending that time? Do you want me doing paperwork? Or do you want me checking relay settings? What are the vital few things I should do? We all have to prioritize. And we have to learn from analogous industries. We have Mr. [Christopher] Hart here to help us out with that. I think there is a lot to learn there. We must align practices with standards and standards with practices. We must make the most of opportunities to share, like we are doing today.

In terms of priorities, we must make the best use of limited bandwidth and communicate clearly. This is something we need to do a better job of internally at LCRA and also externally between ourselves, regional entities, and NERC. We cannot just keep dumping more and more requirements on folks. We need to have a way to manage that, and I think NERC is now aware of this. New standards need to be

formatted for readability, understanding, and a commonsense approach. We must ensure that time is spent on meaningful technical work and not just paperwork. In other words, does NERC want me filling out RSAWs or checking relay settings? There is probably a need to do both, but there must be some acknowledgement that, at the end of the day, you can only do one or the other well. That is a fact.

In terms of learning from other industries, such as medical, aviation and aerospace, transportation, we should recognize that those also have high risks and exposure, have good and bad actors, and have complex problems. There is a lot to learn there. When is the last time you drove through an intersection and the lights in different directions were both green? Has anyone *ever* seen that? It is amazing that the audience in the room has probably driven through millions of intersections, and we have never seen that. What is that misoperation rate? It is awesome. How do they do that? Is it simplicity? Is it hard-coding things? Is it focusing on just doing your job and not all this other communications protocol stuff and other fancy things you can do? Is it getting back to basics? As I go through street lights, I think of how they are very similar and interesting, and I realize that there is a lot to learn from analogous industries.

With respect to alignment of standards and practices, consider that standards are written by committees. As with all good compromises, nobody may be completely happy with it. But a good standard should be common sense, align with industry norms, and be based in reality. When I was designing my first relay panels back at SRP, I was trying to be really efficient in terms of fitting everything on the panel. We did not have standards at the time, but I made a pretty good panel. But I put the lockout relays at the 7-foot line, and the technicians did not really like that. I did not use common sense. No one wants to be jumping up to reset a lockout after it rolls. The same is true with standards. You cannot write standards in a vacuum, and you have to allow time to get good stakeholder input.

Sharing is defined as the joint use of a resource or space. There are a lot of benefits to sharing. Sharing forces you to know your stuff. When I was a peer helper back in high school in a math class, the experience forced me to learn the geometry material (even though I was in calculus at the time) a lot better than when I took the class myself the first time. Sharing forces you to know your stuff because you have to get up there in front of people and talk about it. It positions you to learn from others as well—it is a two-way street. When I go to a conference and talk about our misoperations, inevitably there is a discussion later at dinner or in the hallway where I learn something as well.

Sharing engenders goodwill, which we at LCRA saw mattered in our self-report case. We need to think about opportunities to share. There are a lot of working groups out there, industry presentations, sharing of best practices and horror stories. There are a lot of lessons to be learned. Even asking questions can be a form of sharing. But safe harbor matters, and Marty [Golden] is going to talk more about that.

Thank you all for your time.

III. A SHIFTING EMPHASIS FROM CHECK-THE-BOX COMPLIANCE TO EVENT ANALYSIS AND MORE

Michael "Mike" Moon,

North American Electric Reliability Corporation (NERC)

Good afternoon, everyone. I know exactly what you are thinking. This is a phenomenal conference, and I am glad that we are talking about the regulator, but why did you invite one?

This is a really critical time at the electric reliability organization (ERO) because of changes, shifting emphasis, and what we are learning. It is also critical because of the perceptions, rightfully acquired by the industry, of how they have been treated. *Let me say that again*—we have listened to the industry, and their perceptions of the way they have been treated are partly our fault. One of the signs of a mature industry or organization is the willingness to accept some criticism, to deal with facts and reality, and to figure out how to solve problems. There is a tremendous amount of emotion and baggage associated with the first seven years of the mandatory regime. Regulatory bodies take time to mature. What I want to go through is a little bit of history, to talk about the enforcement that has occurred over these last seven years, and to talk about where we are going and what we are learning because we are listening.

Standards can be good or bad. When it comes to implementing and enforcing them, sometimes there is some creativity. But on the compliance side, there is a responsibility of the enforcing agency to exercise good auditing principles, and that is one of the areas we are working on. We have gone back and taken a critical self-assessment of how we have done business, focused on an event, and found out a lot about our systems. You may have silos in your organization—so-called “cylinders of excellence”—but we all have to break down systems and find why things are not working. There is a specific case study I will explain quickly to demonstrate. I will talk about event analysis and reliability assurance, how we do compliance enforcement, and how we are trying to take the burden off of you.

If you go to the NERC website, there are a couple of pages on our history. I will highlight a couple of things. We are an event-driven industry at every level, including the political level. When you go back to 1963, we formed an industry committee. That was generated because of political discussions regarding what was going on with regulation and how to hold people accountable. The industry agreed to get together and form a committee and start helping ourselves, and that is a good thing.

Then you had the 1965 blackout, and the political rhetoric really started cranking up. The predecessor of FERC said we needed a council. The industry tried again to stay ahead of things, and NERC was established as that council. Then, unfortunately, another blackout occurred in 1977, which led to another round of the political machinations, calls for greater accountability, and customers calling their congressman saying, “I should have power all the time. What is the problem?” There is an action and a reaction. Then we had the 1996 event in the West, and the 2003 Northeast blackout occurred, and all create reaction at a political level.

The Energy Policy Act is the result of a few big blackouts. It is about accountability. But one of the things that we are learning is that accountability should be based on a just culture. I do not see anyone with malicious intent, willful misconduct, gross negligence, or economic decision to violate, yet we began with a very heavy-handed enforcement. It has been said that there is nothing worse than an ill-informed regulator. If we do not have good data, we cannot have a good policy discussion, and we cannot arrive at a good decision. It really is that simple. Yet in June 2007, mandatory and enforceable standards became effective. And, in October 2007, the Transmission Availability Data System was approved. This means that we started a data gathering process after we already had mandatory reliability standards.

The version zero standards came from the original operating guidelines that the industry had been using. The challenge for engineers was that they would talk to one another about the guides and say, “Oh, I know what you mean.” But, once something becomes a legal instrument, which is what happened with the standards, then who gets involved? Lawyers. Lawyers are not engineers. One of the real gaps was that we do know how to plan and operate, but we did not articulate clearly and draft a clear legal instrument. That is one reason for the churn that Kris mentioned. We are now looking at how to improve those. Just last year, we hired five independent experts. One of them is to review all of the standards for content and quality. We are looking to retire standards that are obsolete, and we are looking to improve the ones where the quality is not there.

In 2008, we saw a wave of self-reports. Over 70 percent of the possible violations are self-identified by the industry, and that is tremendous. Think about that—you are turning yourselves in. I will tell you that this is one of our biggest and best arguments when we go before FERC and say, “This industry is doing the right thing. They are self-identifying and self-reporting. So we do not have to be a heavy-handed enforcement authority.” This is where we are going.

In 2008, we also had the Florida blackout, but really the most critical thing was the settlement in 2009 with Florida Power and Light (FPL). What was the most significant result of that settlement? No, it was not \$25 million. In the last three pages, two of the commissioners, Moeller and Spitzer, opined and said, “We believe that the outcome of this settlement is just, however, *we do not believe that the process afforded the industry an opportunity to learn.*” You had FERC commissioners saying that because everything was locked down in compliance space, the industry did not know specifically which compliance standards were targeted, the basis of the issues and alleged noncompliance, and the industry did not learn from it. [*Editor’s note: FPL believes they were in compliance at all times, alleged that standards were ambiguous and subjective, and admitted to no violations in reaching a settlement [3].*] Those two commissioners really set the stage for a shift at FERC toward less investigations. In 2011, following the Southwest cold snap and the August Southwest blackout, FERC did not start with big investigations. In each case, FERC initiated what they called

an inquiry, and they focused on an event analysis report and getting out recommendations. [Editor's note: *Arizona Public Service and Imperial Irrigation District have since been penalized financially by FERC for the 2011 Southwest blackout [4] [5].*] This is why I think the FPL settlement was so important to the industry. FERC acknowledged that we must learn from events and not lock them down in compliance alone.

Fig. 4 shows the early violation history. Again, over 70 percent of the standards violations are self-identified and reported. That is tremendous evidence that you turn yourself in. Imagine if drivers had to self-report every time they did not stop completely at a stop sign or they exceeded the posted speed limit.

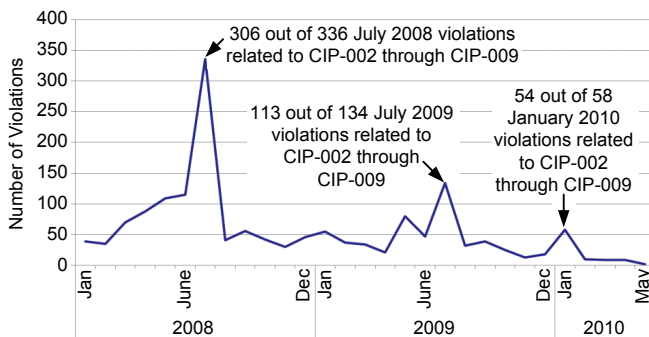


Fig. 4. Early Violation History

The challenge at NERC is that peaks in self-reporting are like waves coming in that have to be processed. When looking at these waves, we consider a couple of parts. Was the standard really understood? Did the industry self-report out of an overabundance of caution? Obviously, processing these waves of self-reports can be cumbersome. In January 2010, NERC President and CEO Gerry Cauley decided that we must do something different.

Auditing is as much art as it is science. It is a profession, just like engineering. And when you talk about check-the-box compliance that Kris mentioned, one problem early on was that we took a bunch of engineers and said, "Oh, by the way, you are now auditors. You'll be fine! Here is the checklist." Likewise, we said to the industry, "Here's a standard. Here's a checklist. Here's an RSAW. Did you violate anything?" Again, some 70 percent of violations were self-reported. Early on, it was never a matter of judgment, but rather if you find a violation, process it. We needed to rethink this check-the-box mentality because that is not the way to do auditing, to administer an enforcement program, or to run a highly technical and complex industry. Fig. 4 is a chart that really began to drive that home. People were just reporting violations, or we were just finding things in audits. That is not the purpose of a reliability organization. The purpose should be about reliability, not enforcement.

As the regulator, those early hundreds or thousands of violations were processed all the same way. Some were administrative, like in FAC where it says that your process will state that you will identify your most limiting element. That is an administrative requirement. But that was also a

potential violation (PV). This is ridiculous, and we have got to do better than that. That has nothing to do with reliability. If you have a good process, but you did not have a statement verbatim within your documentation, that is not likely to impact reliability. But, in those early days, whether it was an administrative or a system operating limit (SOL) violation, NERC processed all of them the same way. On our side of the fence, that led to lots of hours, money, and lawyers. Our business is not about lawyering. It is about electricity. As our case load was growing, the processing time required to dispose of each case kept growing and growing. How do you reduce the case load? We started to streamline this process, from the full proceeding notice of penalty (NOP) to the abbreviated NOP to a spreadsheet NOP.

But so far, all of this is a lot about efficiencies for the ERO. We were still not giving registered entities better efficiencies. That was when we went to find, fix, and track (FFT). The idea was to find ways to dispose of things really quickly on an Excel® spreadsheet. And then finally, we shifted to our risk-based concepts. What is the risk to the grid of each violation? For many violations, honestly, there is little to no risk. We should allocate resources commensurate with the risk. If something is low risk, the process should assign a \$0 violation, or dismiss it altogether, and move it along quickly toward corrective actions at the registered entity.

When we began talking about risk and reliability, we decided to re-energize the event analysis program. When the mandatory regime started, what happened? *All the event reporting dried up.* How many of you remember the Disturbance Analysis Working Group (DAWG)? Every year, they would put out a report of events and disturbances, complete with detailed schematics, sequence of events, and root-cause analysis. All of that stopped. NERC did it for 30 years, and then it all stopped because of the compliance fears that Kris and David point out, because of the fears of enforcement. And what happened? Nobody was learning. The FPL settlement really drove that home. So we re-energized the voluntary event analysis program in 2010. We also looked at how to help you meet compliance obligations and implemented the annual self-compliance program. The goal here was to help entities with their compliance obligation and to give credit when entities do these things. Giving credit is really critical.

In 2010, we started two field trials of the event analysis program. We drafted a process with industry stakeholder participation, which was approved by our board, and authority for making revisions was delegated to the NERC operating committee, also made up of stakeholders. Since December 2010, over 350 reportable events (NERC Category 1 through 5) along with some 1,500 noncategorized events have been reported by the industry. It is a very successful program, and we are learning a lot. In 2011, we began cause-coding, using a process adopted from the Department of Energy (DOE) by which we can analyze events, slice and dice root causes, do analysis, and look for trends.

In 2013, we started having conversations with the registered entities about their events, confirming the root and contributing causes, adding some rigor to our process and data. This has been hugely impactful, and again, it is another indication of the industry doing the right thing. I love to be able to go to FERC and give them statistics like this and prove that the industry is doing the right thing. Through all this analysis, we are identifying reliability risks. I am going to point out two that we found. But you cannot analyze for trends unless you have a process in place. You cannot fix problems unless you know about them. And you cannot preclude the big events unless you focus on the little precursor events, too.

Fig. 5 shows a case study one-line diagram. Rich Bauer at NERC was our lead engineer and analyst on this case. After seeing a couple of breaker failure events over the course of a few months, he did some research. Rich discovered six total events, all involving the same breaker manufacturer and model. After calling the manufacturer, Rich learned that they had produced a service advisory in 2010 dealing with a material defect along with improper torque specifications. The advisory may not have been widely disseminated, or if it was, and in spite of the manufacturer's best efforts, it was not picked up on by a number of entities. This a good example of finding a reliability risk through analysis of the shared event data, and this is how we will solve problems.

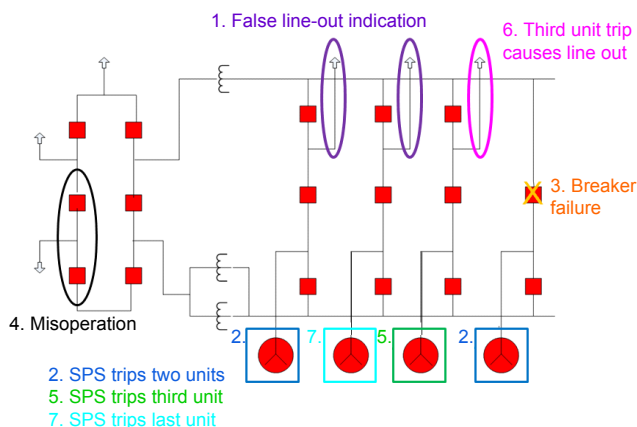


Fig. 5. Case Study One-Line Diagram

In order to identify problems, you have to have data. When we started having conversations with entities in 2013, we knew that we would have a big hurdle to overcome because the industry was skeptical. Many regional and registered entities did not want to talk to FERC. Those first few calls that we did in 2013 began the same way, with me, as the department head, saying, “I am Mike Moon. I am the senior director at NERC, and we are here to talk about event analysis—the engineering, the technical issues, what happened, and why it happened. This is not a discussion about standards. This is not a discussion about compliance. We will end the call if that is what you want to talk about. We want to talk about engineering. I give you my word that there is no one on this call here at NERC who deals with standards, compliance, or enforcement.” Even so, over the first few months, people were very leery. But, over time, it took off.

We had one call early on in which there were 12 representatives from an entity that regularly did not talk to each other—a system operator, a planner, a manager, a supervisor, a compliance person, and a lawyer. After about 20 minutes into the call, the lawyer says, “This is really boring, and I’m going to just drop off since you guys are talking engineering stuff.” That was awesome! We took a little bit of success from another call when, after facilitating the conversation with about eight registered entity personnel, they took over the conversation and worked through all the issues, determined root cause, while we simply listened. At the end of these calls, we confirm the root cause and the contributing causes, and then we do a report. It goes back to the entity for a crosscheck, and after they approve the report and the cause codes in a collaborative way, it is then entered into our system for analysis. This has become a critical part of what we do.

One of the ways we identified the problem with our heavy-handed enforcement is through looking at all the processes and procedures used during a few significant case studies. Fig. 5 represents a significant Category 3 event due to the loss of over 2,000 MW of generation. Obviously, the higher the category, the more serious the event and the more we pay attention. The first thing that happened was a false line-open indication due to a relay output contact wiring problem. That, in turn, caused a remedial action scheme (RAS) to trip a couple of units. A breaker failure occurred next, due to the manufacturer’s problem mentioned earlier. An adjacent line terminal misoperated, and the RAS scheme further acted to clear more units. An event like this has several primary effects, and while they may happen close in time, one part of this event may not have caused the other. Regarding this event, specifically, the entity was prompt with their notification. Their initial event analysis report was submitted within 10 days, as required. Within 60 days, NERC received a higher-level event analysis report, and it was phenomenal—details, timelines, schematics, everything. Within 30 additional days, the entity did their compliance self-assessment. It was also very detailed, addressed critical requirements, and they self-reported one violation. The one violation, by the way, had nothing to do with the event. But, in the course of their review, they found an unrelated planning issue, and they self-reported it. They did all the right stuff. What did the ERO do? The self-report went through the process and led to a fine and a notice of penalty. That is the bad news. The good news is that because this is a higher-level event that attracted more attention, we really got into the details, and we found that what happened on the event had nothing to do with the standard violation that was self-reported. This became information used internally at NERC enforcement to say, “This is wrong. They need more credit for good event analysis. They need more credit for a voluntary compliance self-assessment. They need to be recognized for this, not punished.” We were able to use this case to promote improvements internally.

All of this takes information and sharing. When an event occurs, registered entities are encouraged to do two things—produce a good event analysis report and produce a good

compliance self-assessment. We encourage entities to work with their region in a collaborative way. If we work through this and it is good, how do we give you some incentive credit? Now, we are doing close-out letters. A good event analysis report and a good compliance self-assessment are both indicative of your commitment to reliability, your understanding of your compliance obligations, and the good work that you are doing. A close-out letter says this and can be used favorably in the future to adjust your compliance monitoring. I tell people, “I don’t worry about the people that report events. I worry about the organizations that do not report events.”

All of this leads to where we are going with compliance. If your company does good event analysis reports, good self-assessments, and you work with the region in an up-front, open, and honest way, we believe those are evidence of good internal controls. That is what the reliability assurance initiative (RAI) is about—improving your processes, achieving continuous improvement. In the future, when we go in and assess your entity, your risk goes down, and your future compliance monitoring can go down, too. FERC has this in an order to allow maximum credit for self-reporting.

At NERC, we continue to mature. As I consider the title of this discussion, “Reinventing the Relationship Between Operators and Regulators,” I will tell you that most of that burden is on us, the regulator. We have listened to the industry, we are working hard, and we are trying to focus on reliability. We are focusing on data and analysis so that we can move the emotion out of the discussion and fix problems. Finally, we are working to establish a just culture and treat you fairly. It is not a criminal activity when some of these possible violations occur. Thanks very much.

IV. REFOCUSING ON RISKS TO RELIABILITY

Mark Henry,

Texas Reliability Entity, Inc. (Texas RE)

I am going to cover some of the same ground as Mike did, but I am going to offer you a different perspective on it. First, Texas Reliability Entity is responsible for taking care of reliability rules for ERCOT within the state of Texas, along with some other functions. I no longer work directly in compliance—I did for many years—but I still hang around those people, we work together, and we talk about what is going on. I want to give a little background on what we have seen in Texas and give you a sense of where the program is going.

We are working very hard with a couple of the other NERC regions to spearhead changes in the compliance program. I will not disagree with the things that Mike said—enforcement has been very heavy-handed for the first few years. We recognize that. We are trying to change it. It may not have been as heavy-handed as some people think. But there is obviously lots of room for improvement in the program, and we need to get back to our purpose. We have had three names, but one name that we never got was “Texas Compliance Entity.” It has always been about reliability, in some form or fashion. We were part of ERCOT, and we sometimes have to

remind the people in ERCOT that the *R* stands for reliability. It is in their name, too. ERCOT is our independent system operator. I am very proud of the work they do, and they have a huge responsibility. But they are also one of the entities we are charged with keeping an eye on.

Within the state of Texas, there are about 23 million customers in the ERCOT region. Texas is actually big enough to have parts of four NERC regions within the state—Texas RE, WECC, Southwest Power Pool Regional Entity (SPP RE), and SERC Reliability Corporation (SERC). Texas RE and ERCOT operate asynchronously from the other three regions, and that is an important point that I want you to keep in mind. Some of you may not realize that. We are an island here in ERCOT, which comprises most of Texas, and there are some things we are concerned about here that you may not be concerned about in the Eastern grid, where they have ten times the number of rotating machines and ten times the megawatts flowing. In the West, they have three times the mass that we do in ERCOT. That is important to remember when we talk in a moment about a particular situation that we encountered.

We have about 41,500 miles of transmission right now. We are adding lines in Texas. Some places in the country have a lot of trouble doing that, but since we have all these windmills out in West Texas and we need to bring that power into the load centers, we have had a big project to do just that [6]. We have about 74 GW at peak that we think we can generate, and we are going to need somewhere around 68 GW when it gets to those hot days in August this year. We hope to have a couple more gigawatts of generators joining us this summer. Resource adequacy is a big issue here. Interestingly, there are no NERC standards about resource adequacy. We are not spending enough time, perhaps, talking about that. Granted, there are lots of other people that are talking about that. But not everything falls into NERC’s compliance jurisdiction.

The PUCT also has responsibility for reliability, as well as the markets in the state. We actually do some work with them, under separate contract, looking at rules that are created here called ERCOT protocols. Just like the NERC standards, those protocols are developed by stakeholders. Unlike the NERC standards, they are mostly about dollars, settlements, and payments. But there are issues about reliability in those protocols, too. They go into more detail sometimes than the NERC standards do, and they are very specific to what happens in ERCOT. We are engaged in some of those.

For the most part, most of our time and effort is spent on NERC issues. NERC is in a unique position here. The authority that NERC has comes from FERC. FERC does not have jurisdiction in Texas over markets. With the Energy Policy Act of 2005, reliability rules at the federal level (and involving Canada, too) that NERC comes up with are enforced in ERCOT through Texas RE.

Let me go back to the turn of the century, so to speak. ERCOT used to be split into ten separate control areas, each trying to take care of their own customers, which were vertically integrated utilities for the most part. In time, that is at the far left of Fig. 6. Recall that ERCOT is an island and

that we are very concerned about frequency here. We cannot draw a bunch of power from our neighbors in the short hand. We have an issue, so we stay on top of that. Back before we went to a single control area, our frequency deviation was in the neighborhood of 15 mHz. Our target was 20 mHz, as a part of what I will call a prototype standard. We then went to the single control area model in ERCOT and issued instructions to generation scheduling entities. Instead of having ten areas each trying to manage their own in-and-out flows, ERCOT now did this for its entire area. The beginning of this time is the white area between 2001 and 2004. You might wonder why it is white—we did not go black! We *lost* all that data over time. And I keep this up here because this is still the slide that we report to some of the different groups within ERCOT to show how things are going. At the time, there was not a great deal of concern about the frequency deviations, which doubled to the neighborhood of 30 mHz immediately after going to a single control area. I did not go back and sketch it in because I thought it was worth talking about why that data was not there. But there was very little concern about the risk associated with the larger deviations in frequency because we did not go black. We needed to understand what was going on here. But most people were too busy thinking about settlements, how the new market was working, and certain signals that were or were not coming in. It was hard to get any traction on discussing frequency deviation. We were very fortunate that we had three companies that were very concerned, and they were willing to bring the issues forward.

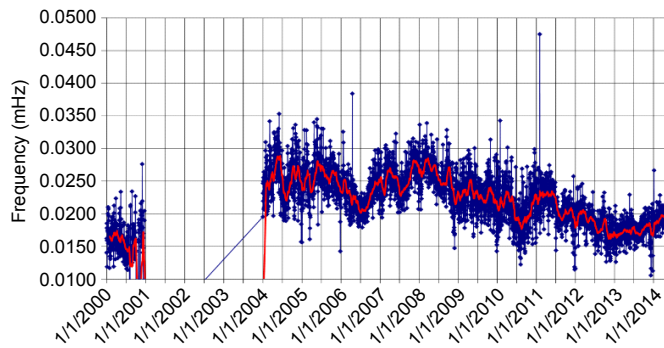


Fig. 6. Frequency Deviations in ERCOT

The chief operating officer of the ERCOT region said that frequency control was as good as it has ever been, and he just was not getting the message because it was a lot worse (based on an established measure, the NERC Control Performance Standard 1). Even still, not too many people cared. What was ERCOT’s responsibility? ERCOT does not control generators. They send signals, and generators have to act. We had no mandatory rules at this time on the NERC side. On the PUCT side, we had some performance expectations in the market rules, but at the time, staff focus was on economics and markets. So the ERCOT organization was not policing things. Again, we were fortunate to have three organizations—one was a pretty large investor-owned utility, one was a rural cooperative, and one was a small municipality—step forward and help us. We worked with them, we found out where the

problems were, and we addressed them, and gradually, we got others to get in line. Eventually, this got dragged up to NERC in some technical committees. Again, there were no mandatory standards at the time. This was all voluntary. We finally got an agreement that things were going to be changed. We hired a consultant to overview the situation. They agreed that for our purposes, we could relax a little bit but that we still needed to do something or else we were going to go black sooner or later. Remember, we are not going to get emergency power from Mexico or Oklahoma.

Things slowly started to turn and improve. Once we got new rules approved and established, we still had to go back to those individual generators. There are no mandatory rules on the NERC side for them, even today, in the area of ancillary services. It is generally to their advantage now to follow their schedule more closely because the rules have changed. They even had a point in time where those that performed well were paid by those that did not. So there are different ways to approach rules and to meet your obligations, but this took a very long time. It was after this period when things started to turn and we started to see frequency deviations go back in the direction of where they were before. This was a risk, and it was not yet reality in terms of actual problems on the system. In Pennsylvania, in New York, in 2003, they had an actual problem. After that blackout, it took two years to get a law enacted, the Energy Policy Act of 2005. Then, two years after that, we had mandatory compliance on the NERC side.

At this point, we put most of our efforts into enforcing those rules. We established a program, and we are all about process. We quit really paying attention to reliability questions in my little part of ERCOT. It was not too long before it was decided that we could not be a part of ERCOT anymore, so we became an independent division. This is because some of the rules apply to ERCOT as reliability coordinator, balancing authority, and transmission operator.

In Fig. 7, you can see that within the first year or two, there were not a whole lot of violations. Things picked up. We have had about 1,000 violations, a little shy of that, year to date 2014. Like Mike told you, most of issues are self-reported. In our case, about half over this time period were self-reported. Lately, it has been more in the neighborhood of 75 percent, so Mike’s 70 percent figure today is realistic for us. Different regions may have a little different story. I think a few regions have written more violations than us, and there are some that have written fewer.

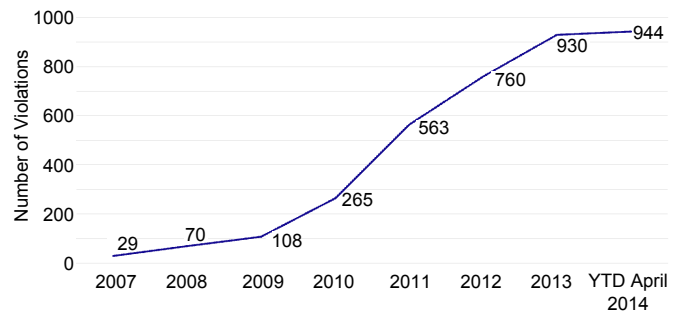


Fig. 7. Standard Violations Within Texas RE

Self-reporting has always been important. Even when we go do an audit, we depend on people bringing things together. We are not pulling emails out of computers looking for things. We have pretty good information about the power system, but we depend on people cooperating, even in an audit.

What is driving those nearly 1,000 violations? Most of them fall into a relatively small group. I forget what the count is, but it is somewhere above 1,000 requirements if you bust them all down. There are not nearly that many standards. But most violations come from a relatively small group, and most of these things are fairly minor. See Fig. 8.

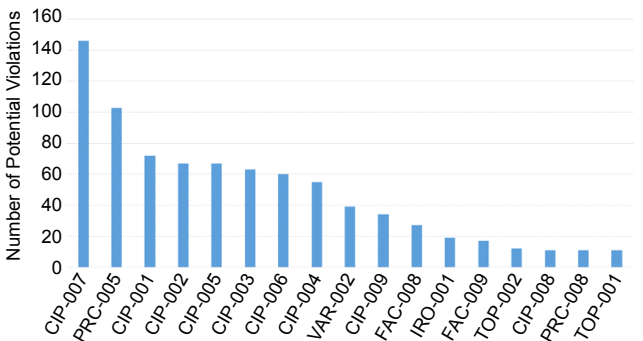


Fig. 8. Standard Violations Within Texas RE, 2014 YTD

The largest one in Fig. 8 is critical infrastructure protection (CIP) CIP-007, a cybersecurity standard related to security management topics like keeping up with your ports, access, and passwords. Everybody makes mistakes with that, you get behind, and something slips. The way the regime that we have works, these are violations. Even though a lot of them are self-discovered and reported, they are still violations. So those are going to move through the process. The next largest item that a lot of you are going to be familiar with deals with protection system maintenance. Again, if you get behind on one of your devices, it is a violation; whether it is a CT—although we still wonder just what kind of maintenance you do on a CT sometimes—or something else, it is expected. The standard was written by industry folks, and people wanted those things to be checked and examined. So that is what we have been doing. Those things move through the system. The third one, CIP-001, is particularly embarrassing to me. A lot of people got written up for not having the local FBI contact’s phone number. It is part of the rule! It is in there. Fortunately, that is one that is disappearing. As was mentioned before, part of the overall process is to look and ask, “Do we really need these standards? Or are some of these covering things that are not important?” Some 86 percent of our violations in Texas come from these standards, and almost all of these things are relatively minor, almost administrative matters.

The big ones, and we have not had too many big ones, show up way out in the parking lot to the far right of Fig. 8. I guess, in terms of how frequently they occur. Folks are doing a good job of running the electric system here. They might need a little nudge here and there, but it is not a pressing issue.

So what kind of concerns do we hear about from the industry? [Editor’s note: Fig. 9 shows the slide used during this point of the presentation.] First of all, weakness in

standards. One indication of a weak standard becomes apparent when we have a rash of relatively minor violations self-reported. Getting those standards changed is not a quick process either. This is something that we want to keep working on.



Fig. 9. Major Concerns About Today’s Compliance Process

Zero defect tolerance—it has to go; it is going to go. There is no sense in trying to waste the time that we have trying to process some of these things as violations.

NOPs are very lengthy and detailed documents because they keep on going back and forth between the regional entity and NERC and then between NERC and FERC. This continues until the FERC lawyers understand what the NERC lawyers told them what had been written by the Texas RE lawyers. It can take a long time for these things to circulate and finish out. Violation resolution can take a long time to get done. It is not always that way anymore, as we have started to address that.

Another concern is just the way we go out and do the assessments. I call it “dump truck” audits. I do not know if that term has circulated, but basically, we have a big list of standards, and if you are signed up as, say, a generator owner, then there are a bunch of things that you need to do even if they do not all fit your situation very well. The auditor is going to show up and ask about every one of them. We do not show up that often—there is a fixed cycle—but then again, there are some functions for which we show up a little more frequently. There is not a whole lot of thought about what a company’s reliability risk is, either in terms of where they sit in the grid or in terms of how they have been performing in terms of event analysis, self-reporting, things of that nature.

Mike touched on this one, which is very dear to me—we were just not sharing information. He talked about the Florida event in 2008, a big blackout. I would have loved to have known what they learned there in Florida, and what they were expected to do, and what we might have applied to what we do here in Texas. But it is a private settlement, and none of us ever heard about it. That sort of thing is a lost opportunity. Otto Von Bismarck said, many years ago, or at least he is attributed to have said, “Fools learn from their mistakes. Wise men learn from the mistakes of others.” That is what we want to be, a room full of wise men.

The Florida case is also an example of the inconsistency in auditing and regulatory review. We have a lot of issues to be

figured out with FERC about how things are done, and some of that is justified because the regions historically did their own thing and had their own way of looking at the world. Well, if we are going to be fair about all of this, we have to line up with each other. There has been a lot of work over the years to improve consistency, and there undoubtedly is still some work to do. Every person who audits is different. But now, the auditors go through some extensive training together, and that is being ratcheted up as well.

The bottom line is this. Even to the extent that Mike and I try to tell you that *you* wrote the standards, there are people that go to committees and pressure the NERC board to reform the program and deal with these issues. We are all in this together, and it is about reliability. We all want to ensure that we are getting what we pay for because we know we are paying a lot to get these things done.

So here are the changes that are going on. Mike described the RAI, and the idea is to get rid of some of those problems that we talked about. It embraces the concept that one size does *not* fit all. If you sign up for certain functions, assuming we still have to keep those functions as some of them may even go away if not necessary, we are going to customize what you do based on who you are and where you fit into the power system. Instead of looking at every single instance of violation, we are going to focus on controls, on how you do your relay maintenance. We are going to talk with you more about the process that you go through and not be so tied into whether you got that one relay at that one substation tested per the schedule you have documented. Cyclical audits, things of that nature, that are done once a year, as well as asking companies to self-certify on all the standards that may apply to them—that can be changed, and it should be changed. We should lessen the burden and look at things that are important. The last thing is sending everything, every violation, to enforcement. Well, that is foolish, and we do not need to do that.

Just to show you that we have started on that one already and that we have made good progress with that, we have something we call FFT. It is supposed to simplify how we do our calculations. We had about a ten-month backlog within the region at the beginning of 2013. Now it is down to two months. Once done, our stuff goes on to NERC. They have done very well, too. Their backlog is one month, and they are working with eight regions. So we have worked through this by saying that certain things can be streamlined, and many cases move through and generally have no penalty. There is another class that we move through on spreadsheets. There are not many that have to have a lengthy legal document describing what was done and how it was managed.

So one of the key components of this overall effort is streamlining things and only spending time on things that really matter. There just are not going to be that many issues that are going to rise to that level of needing enforcement. Penalties really have not been that big of an issue anyway. We have had about \$2.4 million of penalties associated with those 944 possible violations in 2014. Again, a lot of the violations were dismissed. The average penalty is around \$4,000. Now, I

can think of better things to do with \$4,000 than send them upstream, but we have not had \$1 million per day down here. The biggest violations here have not even approached that. To be sure, it is a big bat that is being carried around. But the reality is that there has been some temper on how these things are applied. The last piece of this has to be standards development. Again, we know we have to go back and have a feedback loop on how things are working. We have to make the effort to fix gaps in the standards that are there. There is a move under way to eliminate things that are not productive, are duplicative, or are just administrative. There is another place for that.

The key concept, though, is to look at risk and how risk factors into what we do. We need to get stakeholder buy-in on moving forward with this. We feel that consistency and transparency have been keys for NERC and all the regional programs for some period of time. That is not going to stop. As a matter of fact, if anything, we probably need to improve our outreach so we do not fill your inbox like Kris was talking about. But the information needs to be available to you about what is going on. Risk-based compliance is hitting the right level, pure and simple. It is making sure that we focus on areas of concern. We have to be thinking forward, not backward. A lot of violations that we wrote up in the past were for violations that happened three or four years prior because we have an audit cycle. There is no reason to dwell on something that has already been fixed. If you have good controls and you managed your problem, then it is actually a good thing if we do not hear about it for a while. We just do not want to be reading about these problems in the newspaper—you have to think about it that way. I have touched on inclusion and outreach. Again, we have got to have the industry involved in this.

I want to go beyond that to a culture of reliability excellence. This was the catch phrase of the gentleman Tom Galloway who is now in charge of the North American Transmission Forum. We need to get beyond just thinking about compliance. That has consumed us in ways that I never would have imagined early on, back when I was one of two people working on the pilot program on compliance at the turn of the century. Then one quit, so it was all me for a little while. It was different back then. We always thought of ourselves back then as a kind of inspector, going around talking to people. The audit reports that we wrote in those early days had a component about which standards, or proto-standards we will call them, we looked at, but we also wrote about things that we thought one could have done better. We wrote about things that we saw over at the other shop that could have been implemented here. We quit doing all that in 2007. I think that is coming back, to some degree, within the compliance space. But more importantly, it is going to be in other spaces. As a registered entity, you are doing an excellent job managing these things, and to the extent that the standards are clear and that you can understand them, you are applying them, evaluating yourself, turning things in, and fixing problems. But on the reliability excellence side of things, we have to be able to *talk to one another* about best practices. We

have to have a margin well above compliance. Standard compliance alone is like barbed-wire fence posts. Unless you string something between them, all the animals are going to wander off. So we have to manage our system but operate at the higher level at which we are capable. Continuous improvement—you have probably heard that 50 times at this conference—it will not stop there.

One of the areas for continuous improvement is to look at events. Mike talked about this, and I just wanted to touch on this briefly. February 2, 2011, is a day that I will never forget. Actually, that began a period of several months that I will never forget. We spent a lot of time going through events. We had about 15 GW of generation that tripped offline because things froze up or things would not start or we had to derate because of something else that was jammed shut because of icing or other related problems. See Fig. 10.



Fig. 10. Winter of 2011 at Texas Generating Stations

There are no NERC standards that fit this incident directly. We never did a compliance investigation purely on this. We have done some in the past that were so ugly I will not even talk to you about them. But in this case, the end result for us was that we had 52 companies of the many that we talked to that submitted to us a voluntary lessons learned report. They all shared something that they did as a result of this event, something that they improved upon. We consolidated those with NERC, we worked with a couple of other regions, we worked with industry stakeholders through the NERC operating committee, and we wrote a guideline document and published it. Then we bugged the heck out of people: “Are you using that guideline? Is that guideline any good? What can we add to this guideline to make it better?” We have worked with the ERCOT independent system operator (ISO) and made site visits to generators, asking them, “How is your heat trace working out there? Do you have any insulation gaps? Are you getting all of your enclosures heated up? Are you aware of a wind shift?” We took all of the things we had been learning, and we took the show on the road.

We had an event this January 6, 2014. It was not quite as cold as February 2011, and we did have a few units trip offline. Some of those trips were due to the same problems,

but the 2014 winter event was a lot better. FERC did not ask to come down and visit places like they did back in 2011. FERC has not asked us to write a new standard to cover winterization of generating stations, and we do not think they will either. We have proven that we can address this problem in another way, outside of compliance and enforcement. As a matter of fact, we do not have many events that reach the threshold that Mike talks about. So we are looking at things in the lower levels, what I think we would call Category 0 events, and seeing what there is to learn and share.

We are going through these submittals that people give us that we never looked at in the past because we were too busy with the process, and we are analyzing what is going on. Human performance is a key factor for us. I think Karl Zimmerman in an earlier session was right—we are somewhere around 50 percent of misoperations having a human error component. [Editor’s note: Refer to Fig. 11 for the slide image used during this presentation.] What do we do about it? We need your input on how we move forward.

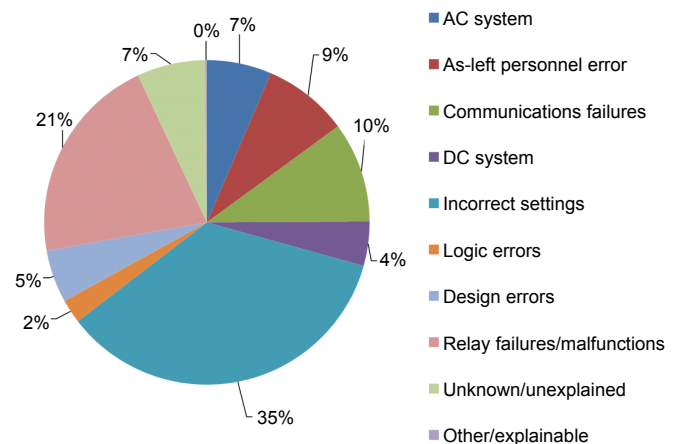


Fig. 11. Misoperations by Causes

If we are going to move forward, it will not be because we fixed this with new compliance rules. We are going to fix this by people cooperating and trying to share information. There is a place for compliance. We are adjusting the program. We are in the middle of that so you may not see as much of that as I would like yet, but we are going to do other things—performance analysis, event analysis, assessments of impact and new reliability risks. In the end, we want to identify reliability risks—after all, that is what the *R* in Texas RE, NERC, and ERCOT stands for—and we need your help to collaborate and get the job done. Thank you very much.

V. LEGAL REALITY CHECK: THE RISKS OF SHARING INFORMATION AND THE NEED FOR SAFE HARBOR

*Martin “Marty” Golden,
Keogh, Cox, & Wilson, Ltd.*

Well, I am sure that those of you who were not thrilled about having a regulator here are even less thrilled about having a lawyer here. I have been a defense lawyer for 29 years, a defense lawyer on the civil side of things, and I am not sure why I was selected for this in the first place. But in

the initial meetings of our panels, when we were discussing this very idealistic sharing of information about misoperations, I was like, “Guys, where are the lawyers? Are you serious?! Are you seriously talking about sharing details and information about misoperations, some of which may have led to property damage and personal injuries, before you even know if there is litigation involved or what the consequences are of this event on that side of things?” “Well, yes,” they answered, “that is what we want to do! And we would like, perhaps, some sort of safe harbor out there to enable us to do that,” they said.

That safe harbor is certainly not there now, and it needs to be a component of whatever it is you are trying to do to make this start happening. So, basically, I have become the “wet blanket” of our panel because, while they have all these great ideals of how to move the power industry forward, I am putting on the brakes and saying *wait*. Is your management really going to let you do that? What are your lawyers telling you? I will bet it is pretty similar to what I am saying.

Of course, the risk here is that while many misoperations have no bad consequences, some have severe consequences. Somebody can get hurt or killed. There can be a loss of production because a plant shuts down for a while. That is when the lawyers get involved. Once that lawsuit train leaves the station, you all are out of control, and your management is out of control. You have lawyers and judges that are in control at that point. I am including the lawyers on your side of the case, but they are not you, and they live in a different world.

What happens once the lawsuit gets filed is that there is now very liberal discovery available under all the states’ systems and the federal rules. They can seek all your documents about what happened, your investigation of what happened, all the email traffic back and forth pertaining to that investigation. These things do not even have to be relevant to the lawsuit. They only have to be reasonably calculated to lead to discoverable information. And if there is any doubt, the court is going to side with giving them the document. So that is the problem you deal with.

So you have lawyers who frankly do not care what happened. They do not care who is right or wrong. In the case of the plaintiff’s attorneys, what they care about is the deep pockets and being able to make a plausible case to a jury, made up largely of uneducated persons (in terms of what you all do), that somebody got hurt on this side of the case and somebody with money dropped the ball on that side of the case. And you do not have to drop the ball very hard because the jury is much more concerned about the person that got hurt. So that is what you are up against. Lawyers have taken a hold of your situation, and they are looking to tag your company, your organization, whatever it is, for big dollars. At this point, you are probably concerned with what management’s reaction is going to be when it comes out that your innocent little email is *the thing* that the plaintiff’s lawyer is harping on in closing argument to justify a multi-million dollar award in favor of his client.

Not to pick on plaintiff’s attorneys, in particular, but I will give an example (and this example happens to be the

particular case where I came in contact with Schweitzer) as to how lawyers on both sides of the fence operate this same way. The Kaiser alumina plant in Gramercy, Louisiana, blew up in 1999 [7]. There was some electrical involvement, but really it was a pure human error case. Kaiser incurred property damage, and because of the total destruction of the plant, this was into the \$200 million range. Several people were badly hurt. Nobody was killed. Kaiser quickly settled with the people that were hurt and paid them three to five times what their case was actually worth. Part of the deal, of course, was that they then had to join in the suit against all of the third parties, including contractors and product manufacturers, who had some sort of presence on the plant. And they all came after those companies together. Kaiser, not a sympathetic party in and of itself, was now tied with the sympathetic parties, those who were injured. And all of the things that I am going to talk about today, Kaiser’s lawyers did ten times more than the plaintiff’s personal injury lawyers did.

So it is just lawyers. It is just what we do. It is like we are the colds and flu of the business world. If you have not caught us yet, you are going to catch us. When you catch us, you cannot cure it, and we are coming back again. So it is out there, and you have to be aware and take certain precautions in order to avoid us.

Now, what happens when the lawsuit process starts? We are not going to be satisfied with the documents pertaining to this particular misoperation. We are also going to subpoena documents related to similar misoperations. Again, the standard is not relevance. It is that a document may be reasonably calculated to lead to discoverable and relevant evidence. So perhaps I can find a pattern through things that have happened previously. So all the reports, all of the drafts of the reports, all the electronically stored information—I am going to ask for it in its native form, including all the metadata. And heaven help you if anybody has deleted any of this stuff, post-incident, regarding a situation in which they should have reasonably known that a claim was possible. If that happens, I now have a spoliation-of-evidence claim, and it refers to the intentional destruction of evidence in a situation where a company knew, or should have known, that a claim was coming. In some states, it can include negligent or careless destruction of evidence. But it can be made to look deliberate, even when it was just someone cleaning out their inbox. That is the situation that you are dealing with.

The next phase, which David and Karl Zimmerman are familiar with, is the deposition. You get sat down four years after you have drafted an email in which you made a few innocent comments about a misoperation. In fact, the email may have been about the fishing trip that weekend, and you just threw in a comment about the misoperation, too. That email then comes up in a word search, it is now in discovery, and years later, you are being shown this email by opposing counsel. He is asking you hostile questions in a less-than-pleasant manner, and he is expecting you to explain a lot of stuff that you forgot two days after you transmitted that email. That is what this process involves. It has been likened to

proctology and a lot of other things that we cannot mention here.

So what safe harbors are out there for you now? What protection does your organization have to keep this information in house, to prevent its disclosure to hostile attorneys, and to make you feel comfortable creating those documents in the first place when the misoperation occurs? We are talking now about creation of the documents, documenting the information, and the sharing of it with other parties, which is just unthinkable to me.

The safe harbors that exist now are evidentiary privileges. A privilege, if it pertains to a certain document, allows you to refuse to disclose it, and the court will enforce that, notwithstanding that it otherwise fits within the scope of discovery. The document is relevant or reasonably calculated to lead to discovery of relevant evidence, but the privilege attaches, so you are allowed to not disclose it.

Well, the first privilege that we are all familiar with is the attorney-client privilege. The attorney-client privilege attaches to communications between a client and their attorney and legal advice by attorney to the client. That includes members of the client organization—it is not just management, it is employees, and so forth. The problem with this privilege, like all the privileges, and it is where we get into the sharing issue, is it is waivable. The attorney-client privilege is generally deemed waived if a document is knowingly furnished to somebody outside your organization. So if, for example, an email from members of the organization and their attorney copies somebody outside of the organization on that email, knowingly, then there is no attorney-client privilege there. If the privilege attaches, it is considered an absolute privilege, and I will explain an absolute versus a qualified privilege in a second.

Some companies use attorney-client privilege in an effort to shield post-incident investigations. They will put an attorney at the head of the investigation team and say everything goes to and through the attorney. Copy the attorney on everything, and when the inevitable lawsuit comes, we are going to claim attorney-client privilege. Well, that is a fairly transparent device that most courts will see through and not accept. Really, your best-case scenario there is that the true attorney advice contained in these documents will be redacted, will be blacked out, and the rest of the document that contains factual data will be produced. So you probably have not saved yourself anything with this strategy, and if it is completely transparent, nothing will be redacted. I have had cases like that, where we have been able to get everything, and the judge has told the other party, “I do not care about your attorney-client privilege, and I do not believe your good faith in asserting it.”

The next privilege is called a work product privilege, and this one attaches to documents and information that are generated or obtained in anticipation of a claim or litigation. So it sounds perfect for the kind of situation that we are talking about, in which there is a misoperation and in which there is property damage, injury, and reason to believe that

there may be a claim. Right? This sounds like it fits. Well, it is so riddled with holes that it does not fit at all.

First of all, this is a qualified privilege. A qualified privilege is overcome by a showing of the plaintiff that there is really no other reasonable means for them to get the information contained in the document. And that is going to be the case very often when you are talking about your typical organization that has tight internal controls, where there is really no other way for them to get it than to go to the person that generated it or to look at the document itself, or whatever the case may be. The bigger hole with this privilege, however, the main reason that it is not the safe harbor that we desire for this situation is that it applies only when the information is obtained, or the document is generated, in anticipation of litigation as opposed to pursuant to that organization’s usual post-incident policy of investigation and generating reports. And I think that everybody in this room is, on a regulatory basis, mandated to gather such information every time there is a BES misoperation; and those that may not be are probably subject to an internal company policy mandating that. And, when that is the case, work product privilege does not apply.

So that brings us to what may be the most interesting privilege, and that is the self-critical analysis privilege. This has been around since 1970. There was a federal court case called *Bredice v. Doctors Hospital* [8]. Bredice was a medical malpractice case arising out of the death of a patient. Like most hospitals, this particular hospital had a peer-review committee that would investigate anytime there was an incident that occurred at the hospital. There would be comments, frankly made, by the hospital staff on what was done wrong and what procedures could be utilized in the future to negate that. The plaintiff subpoenaed the minutes from this particular committee’s meeting pertaining to the death of this patient. And the court held that those documents would not be produced. The reasoning was that the self-evaluative process and comments that were contained in those documents held a strong public interest in terms of good patient care and assuring that it takes place in the future. It created a four-part test, which was applied in a number of other cases and in different contexts that will sound like something that might be your safe harbor, at least for your internal organization, information, and documents. But, again, it does not help you with sharing across the industry.

The four-part test asks first, was the information the product of a critical self-analysis undertaken by the party asserting the privilege? Two, does the public have a strong interest in preserving the free flow of that type of information? Three, would the free flow of that type of information be curtailed if its discovery were to be allowed in this scenario, in which there is ongoing litigation and potential liability? I think these things cover what we are talking about today for misoperations in the power industry. However, four, *was the information intended to be confidential?* If it was, and we are talking about a purely internal report or document, then this self-critical analysis privilege is an option. But, as soon as you start sharing something with all the other members of the industry in the hope that they will learn something and be able

to avoid this going forward, then you have lost part four of the test and you are not realistically going to be able to claim this privilege.

Now, this has been applied in other types of cases. It has been applied in a defense contractor's assessment of its Equal Employment Opportunity practices. It has been applied to accounting records, academic peer reviews, railroad accident investigations, and product safety assessments. So, above and beyond the issue of sharing to outsiders destroying the privilege, why is this not useful? Why, if you at least keep your post-incident investigation report in house, does this not protect it? Well, once again, this is a qualified privilege. So, if the plaintiff's attorney can demonstrate that there is no other reasonable means of him obtaining that information, then the court is going to require you to give up the document. Again, there may be some redaction of those subjective self-critical elements that are contained within it, but certainly anything factual you will have to produce. There is the waiver problem, and perhaps the bigger problem is that this is a very controversial form of privilege. It has not been officially accepted by many states at all. Many opinions have discussed it and suggested an open-mindedness to it but have refused to apply it in that particular case. There is a specific exception that is relevant to your industry and that is for cases where the government, or some government agency, is seeking the document. Most courts hold that it does not apply to that. Interestingly, in our Kaiser case, before the civil litigation (or really in parallel with it), there was a regulatory action by the Mine Safety and Health Administration (MSHA), the mining version of the Occupational Safety and Health Administration (OSHA). MSHA had jurisdiction over Kaiser and had jumped in after the plant explosion and had subpoenaed a whole lot of documents, which Kaiser tried to withhold on the basis of the self-critical analysis privilege. It was really kind of absurd. I was in that case, and they were just trying to apply this to everything imaginable. This was before the documents were even actually disclosed, and the court was kind of giving them the benefit of the doubt, for the purposes of the argument, and assuming there was some self-critical analysis in the documents. Nevertheless, here is what the Fifth Circuit (the Federal Circuit Court covering Texas, Louisiana, and Mississippi) said in rejecting that privilege: "The Fifth Circuit does not recognize the self-evaluation privilege, and courts with apparent uniformity have refused its application whereas here the documents in question have been sought by a government agency." So that, it seems to me, is one of the big issues that many of the non-regulatory agency folks here would be concerned about. Obviously, it is not just that the lawyers are going to swoop in and file a lawsuit. Some regulatory agency is going to attempt to get these documents, too. So this privilege does not help you at all.

In our discussion of finding a safe harbor that would allow this type of sharing of information, whether we are talking about safe even to the point that a regulatory entity cannot get it or can only use it for limited purposes, I do not know. I think perhaps that goes beyond the scope of it. But we are at least talking about giving protection against us, the lawyers,

and these private lawsuits. The concern, of course, is not just that other people, if it is subject to this discovery process, will not get the benefit of it within your industry because you are afraid to share it. It is that you are afraid to even create it and to communicate it internally within your organization because of the prospect of having to deal with it as evidence later.

In a 1990 case, the U.S. Supreme Court expressed some hostility to this privilege as well but also announced, really, the solution that we need to talk about. This was an employment discrimination case, and certain records were resisted by the defendant on the ground that they were academic peer-review records. It was the University of Pennsylvania that had been sued. The Supreme Court said the following: "The balancing of conflicting interests of this type is particularly a legislative function." And that is the point.

None of the existing privileges do what you need. What you do need is legislation, perhaps at the federal level, and if not, then in all 50 states. It is doable. The hospital peer-review situation that we discussed is recognized in nearly all 50 states, and it is *not* because of that 1970 case that we discussed. It is because nearly all 50 states have adopted legislation expressly approving a privilege for that situation. Hospital peer-review records are not discoverable in any context, and courts are very serious about enforcing that because they have the legislation to back it up. They are not just making it up as they go. There is also a similar situation where the Federal Aviation Administration (FAA) has created a regulatory safe harbor for reporting airline incidents. But that still does not protect those airlines from potential civil liability.

So what do you do until then? What are your options? You are not going to get this legislation enacted in the next year or two, so what do you do about all of this? Do you do nothing when you have a misoperation? Well, it is apparent from our regulators that is a big no-no! There are some regulatory consequences to doing nothing, to failing to report. On the civil liability side of things, there is nothing a plaintiff's attorney would rather tell a jury in closing arguments than they did nothing, they changed no procedures, and they did not try to prevent this from happening again in the future. You are sunk if that happens, so that is not helping your case at all.

I think the answer here is what I call "smart morality." You do the right thing. You do what you need to do in order to be able to look at yourself in the mirror, to be able to live with yourself, whatever your cliché is, but you do it in a smart way. Now, we live in a lawyer-driven society, to the point where we are all afraid to do anything. Look at all the absurd warnings on all the products we buy today. That is where all of that comes from. Each warning has been a product liability hit and a lawyer advising a client that in order to avoid other hits, here is what we need to put on our label. Lawyers certainly have a role in management, but management needs to make balanced decisions that take into account risks, but also take into account doing the right thing.

So what about the *smart* part of "smart morality"? Be aware of the potential for litigation when you are doing all this stuff during your investigation. When you are doing drafts of

reports, realize that the drafts are discoverable, not just the final report. When you are making notes, bear that in mind, especially when you are sending emails.

You know, emails are great, but for whatever reason, we do not talk to each other much anymore. Speaking by telephone is almost a discovery-proof form of communication. Three years later when I am deposed, “No, I don’t remember exactly what I said on that date.” But, if I have an email with all these little details, including some innocent comments, I have to explain every bit of it.

When you are emailing, think long and hard about “reply to all.” Reply to all kills your privilege, if you have it at all, if there are any outsiders on that chain of email. Plus, everybody on that chain of email three or four years later is going to be deposed and asked, “Did you receive that email? What did it mean? What did you do about it? Why did he send it?” And you may not even remember at that point, so be aware of this. Be aware when you are drafting an email of the content, that you can be asked questions about it, and assume you will be asked questions about it, even if it never comes up again. Do not put in flippant remarks. Do not do CYA. CYA says you know something was wrong, but maybe if you make the right flippant comment, the blame will not be cast on you. The plaintiff’s attorney does not care about casting the blame on you, but you will be asked long and hard about it.

Unfounded criticism? Do not put it in the email. And especially, above all, avoid speculation. If you put that in the email, the attorney will ask why you thought that might be the case, and it will suddenly become the case whether it is reality or not.

So let us all work on getting the safe harbor we all need. And until then, hush! Thank you all very much.

VI. COMMERCIAL AVIATION: A REGULATOR-INDUSTRY
COLLABORATION SUCCESS STORY
Christopher “Chris” Hart,
National Transportation Safety Board (NTSB)

I want to talk about how this success story worked in aviation, but I am not going to say that one size fits all or that because it worked for us, it will work for you. In fact, I admit freely that I do not know that much about your industry and what you do. So I cannot begin to tell you whether this would apply to you or not. But I am going to explain the context for us and ask you to consider if it is relevant for you to make a determination whether it would be useful for you in your context.

NTSB—we are the accident investigators. I am not going to go over this in great detail, but that is my perspective. We investigate accidents in all modes of transportation and determine what caused those accidents. Our primary product is recommendations to try and prevent those accidents from happening again. The focus of our recommendations is safety. We do not do quantitative cost-benefit studies. We are qualitatively aware of the cost-benefit situation, but we do not do quantitative cost-benefit studies. What we are created for is to give you, in an ideal safety world, a world in which safety

is the only consideration, what you would do to prevent accidents. Obviously, safety is not your only consideration.

We are created to be an independent agency so that we can create an impartial and unbiased result of the investigation. Typically, in most regulated industries, the regulator is the investigator. So what that means is if the regulator did or did not do something that contributed to an event, then that is not likely to show up in the regulator’s report. At NTSB, we are not a regulator, so we give an unbiased, independent, and impartial conclusion about what happened.

Here is the context for us in our industry, and this is a structure from what I hear that we share with you in the electric power industry. *[Editor’s note: Refer to Fig. 12 for the slide image used during this presentation.]* The structure for aviation is a system of subsystems that have to work together successfully so that the whole overall system will work. The subsystems are coupled, so that if you make a change in one subsystem it will likely have an effect throughout the other subsystems. So the overall system is complex because of this coupling. The system is also high tech, it is always evolving, and we are always learning. These are characteristics that I think you share. As soon as we figure out one technology, we are looking at a new technology.

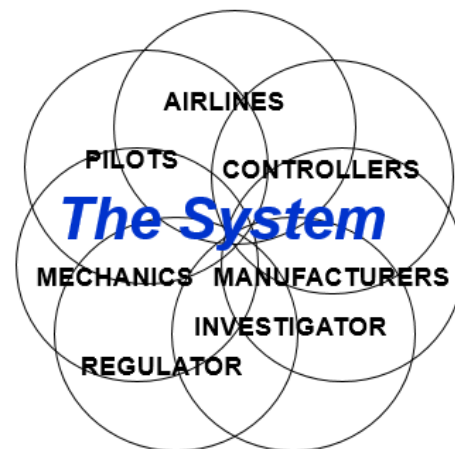


Fig. 12. Aviation Safety Involves Complex Interactions Between Subsystems

What we find in that context is that safety problems are not because of one of the subsystems but because of the interactions between the subsystems. That is good news and bad news. It is good in that it means that the overall system is sufficiently robust so that just one problem alone will not be enough to hurt somebody or bend any metal. The bad news is that it is very difficult to identify one point of intervention and say that if we just fix it right there, then it will fix the problem. This is our increasingly complex system, and from what I hear, you share these characteristics with us. You, too, have a complex system that consists of many subsystems that have to work together successfully for the entire system to function correctly.

So in light of that increasing complexity, we see more human error for three reasons. First, the system is so complicated that it is difficult to design it to be error free. Second, the people who operate the system at the pointy end

of the spear, as James Reason would say, are likely to encounter situations that were not anticipated even by the designers of the system. We do not like the commercial airline pilot of a flight full of passengers to become a test pilot. Engineers anticipated that airplanes would ingest birds, and that is why they designed the engines to do that without exploding. If the engines explode when they ingest birds, obviously the outcome of a flight would be very different. The engineers did not anticipate having an airplane lose *all* of its engines to bird ingestion; however, it has happened in the recent past [9]. So, in such a case, the pilot is a test pilot. He has never been trained to glide an airliner. He has never been trained to land it in the water. Therefore, that means that he has to learn on the fly, excuse the pun, and he has to learn immediately. That is one of the outcomes of more complexity. You increase the likelihood that the operator at the pointy end of the spear is going to have to do something that was not anticipated by the designers.

The third and last but not least reason is a variation on that theme. The people who design the processes, procedures, rules, and regulations also do not necessarily understand the totality of this system and the complexity of the subsystem interactions. That means a lot of your workers who are experienced, seasoned workers will say, “Well, I know the rules say to do it this way, but if I do it that way, I can do it better, faster, and cheaper.” You are then faced with a conundrum. This person who did not follow the rules also did it better, faster, and cheaper. Does that mean we should fire that person for not following the rules? Or should we revisit the rules because this is a well-intentioned person trying to do it better, faster, and cheaper? If you have a person who just does not like to follow rules, that is the person you want to remove from the organization. But if they are trying to do it better, faster, and cheaper, and they are doing it by not following the rules, then maybe it is time to revisit the rules and admit that they do not fit this circumstance.

Those are the three things that we see from increasing complexity. The system is harder to design in a way that is not going to produce error, the operators are going to encounter situations not anticipated by the designer, and the operators are more likely to do it better, faster, and cheaper than the rules say.

We have staff in which we invest a lot of money into training them, who are competent, proud professionals trying to do the right thing. But they are humans, and they still make mistakes. That is the challenge. How do we take these complex systems that have to be operated by humans and do this in a way which we can respond to this reality that there is always going to be human error?

What I propose as a solution is what I call “system think,” which means understanding when something is done to this subsystem how that will affect the other coupled subsystems within the total system. Here is how we did it in aviation. We did it by bringing all the players together. We brought together the manufacturers, the airlines, the pilots, the controllers, and the regulators. Everybody came together to collaboratively work on four things. First, identify the potential issues and

problems. Second, prioritize them. I guarantee you that if this process is any good at all, it will identify more issues that need to be addressed than you have resources to address. So you have to decide what are front-burner issues and what are back-burner issues. Third, once you decide the front-burner priorities, develop the interventions for those. Last but not least, evaluate those interventions to make sure that they are doing two things. They must be accomplishing what you want them to do, and they must not be creating unintended consequences. A huge problem with complex systems is when you make a change here, you are likely to have unintended consequences elsewhere. Identifying and minimizing unintended consequences is a huge challenge.

This was a big shift in the way we think. We used to say that we put a lot of money into training the human and if that human had absorbed the training, then they would not have messed up, so it must be time for punishment. We thought we had taken care of the problem once we punished Joe. Well, you did not take care of that problem—and why not? Because Joe is a human, and humans make mistakes—that is a given.

We had to look at two things. What was it about this system that created the possibility that this mistake could happen? And why could the system not accommodate the mistake without catastrophic result? Then we begin to see what we could do to improve the system. Note that when we explore the system in this context, it does not let Joe off the hook. This is not a get-out-of-jail-free pass because, ultimately, the operator is always responsible and accountable. We do not eliminate that responsibility for the operator. What we are doing is looking at the operator and also looking at the system instead of just looking at the operator and just punishing them, which is what we used to do. This was a huge change in thinking from just punish, punish, punish, to looking at the operator and making sure they are well trained and performing *and* looking at the system and how it can be improved.

Look at the healthcare industry. The Institute of Medicine put a report out in 1999 estimating somewhere between 44,000 and 98,000 deaths every year in U.S. hospitals were due to medical error [10]. That is a huge number, nearly 1,000 to 2,000 every week, and that is pretty scary. That really focused attention on something that people previously did not see at an individual or local level and something that had not received much media attention. This was a total surprise to learn that 1,000 to 2,000 people a week die in U.S. hospitals due to medical mistakes. So what else did the report say? If we keep blaming individuals, we will not get anywhere. We have got to design safety into the system. When I saw that report, I read it and replaced *operating room* with *airplane* and *doctor* with *pilot*, and it looked just like us. That is when I realized that what we were doing is so generic to so many industries, and they are doing exactly the same thing. That is when I started talking to the medical industry, to prevent everyone from reinventing the same wheel, and asking to work together.

I get asked, “How do you aviation guys manage risk as well as you do?” I am asked to speak to many industries—

nuclear power, petroleum refining, healthcare, banking, chemical manufacturing. School boards came to me, and I said, “Why? I don’t get it.” Their analogy was that their airplane crash is when someone dropped out of school in the ninth grade. So all of this is much more generic than I ever knew. That is why I put it out to you and say, not that one size fits all, but to please look at the context in which it worked in aviation and see how much it applies to your context and your industry.

The objective of this process is very simple, and it is two-fold. One, make the system less likely to cause error in the first place; and two, make it more able to tolerate error without catastrophic consequence. Again, this a huge shift from the way we used to do it. Back in the old days, if you looked at NTSB reports, they all ended with pilot error, pilot error. In the 1990s, we realized these pilots are well-intentioned people, well trained, and not only that, they are the first to arrive at the scene of the crash. We were sure they would rather not be there. So what was going on? What was wrong with the picture?

That is when we started looking at the corporate culture and whether there were bigger things besides just the pilot. Well, now we are expanding that even further. Just like you might say that a culture of corporate safety needs to start at the top, now we are saying that industry safety culture needs to start from the top. And who is at the top of that industry? The regulator. The regulator is at the top. That means that the regulator needs to be firmly on board with this concept of improving safety. That is the evolution from pilot error to corporate culture to industry culture. And that is a whole different role for the regulator. The regulator needs to actually play a leadership role in getting and improving the safety culture of the entire industry.

Here is what happened in aviation. We brought together the manufacturers, airlines, air traffic control, labor, and regulator to identify, prioritize, solve, and evaluate. What really led everyone to doing something different and thinking out of the box was that for many, many years, the accident rate in aviation was coming down. This was due to lots of reasons but mostly new technologies. For example, jet engines were so much more reliable than piston engines, so that brought the accident rate down. Simulators then came along, and you can train pilots to do all kinds of things you would never think of doing in a real airplane. Then, if they ever saw that situation in the real airplane, they have been-there done-that, and they know exactly what to do. Simulators hugely brought the accident rate down. Well, that accident rate started getting stuck, leveling out, in the early 1990s. Meanwhile, the FAA was projecting the volume of flying to double within the next 20 years. So the aviation marketing people did some simple arithmetic and figured out that a flat accident rate multiplied by a doubling volume meant that the general public is going to see burning, smoking planes on CNN twice as often. It was probably not going to help to tell the public not to worry because the accident rate is really low. They will not be impressed by that. The public counts the number of events

they see, not the accident rate. That is what scared the aviation industry into doing something different.

Here is what resulted from doing something different. *The aviation industry took that stuck-flat rate and reduced the accident rate by more than 83 percent in only ten years, between 1998 and 2007.* It is because they took this “system think” process, and they fueled it with information from the front lines, from these proactive safety information programs. What is even more amazing is that the way they improved the safety flew in the face of conventional wisdom. You always hear safety up, productivity down or productivity up, safety down. Well, guess what? *They brought both safety and productivity up at the same time.* Think about that. This was primarily a safety program, and nobody was really thinking about productivity. But they improved safety and productivity at the same time. My view on why this process is so sustainable and why it is still going on to this day is because, as much as we safety people hate to say it, *a program is not sustainable if it hurts the bottom line.* Well, they found they can improve safety and help the bottom line at the same time.

Well, guess what else happened? *This collaborative process did not generate a single new regulation.* [Editor’s note: Audience applause erupted at this point.] You know, that is funny because when I told that to the American Banking Association, they actually gave me a standing ovation. After the 2008 financial meltdown, they are facing this host of new regulations. Aviation was already a heavily regulated industry. They already had regulations that say, “Be safe.” So what would be the advantage of another regulation that says, “Be more safe”? That is not the solution. They realized it is not a matter of more regulations, and it is not a matter of more enforcement, and it is not a matter of a bigger stick for the enforcer. It is a matter of trying to figure out how to take this complex situation and respond to it in a way that improves safety. That is what the aviation industry did, and that is what this collaborative process was able to do.

So the moral of the story is very simple. If you are involved in the problem, you need to be involved in developing the solution. Let me give you a couple of quick examples. A ground proximity warning system warns the pilot when the ground is approaching faster than it should be under the circumstances. The first versions of the initial software gave a lot of false alarms. Guess what is going to happen after a pilot gets a false alarm two or three times? They are going to pull the circuit breaker. The only thing worse than not having a warning is having a warning that you ignore because it gives too many false positives. Why would the pilot disable the alarm? The rule is that when the ground proximity warning goes off, the pilot immediately does a go-around—nose up 18 degrees, gear back up, full throttle, and get out of there. After you did that a few times when you did not really need to, because you were actually nowhere near the ground, you are going to start ignoring the alarm and pulling the circuit breaker. By fixing the software and the effectiveness of the ground proximity warning system, it reduced the unnecessary missed approaches, which reduced costs, airplane time, pilot time, passenger frustration, controller time, etc. They

eliminated all of that, and they reduced the warning system complacency, which improved safety. This was a huge success.

Another example deals with flap overspeed. The VP of Safety at a major U.S. airline was trying to get the airline to start looking at flight data recorder information all the time. They were not designed to be looked at after every flight, but rather they were designed to be looked at after a crash. That means you really only look at and benefit from the data once. Well, in the United Kingdom, as early as 1970, they learned that if you looked at it after every flight, you can learn a lot about near misses. [*Editor's note: Comedian George Carlin would refer to these as near hits.*] By studying the data, you could learn what went wrong to cause this near miss and what went right to keep this near miss from becoming a crash. They realized if you looked at it after every flight, there is a lot of information from which we may learn. So the VP of Safety at that airline convinced his bosses, his lawyers, his Chief Financial Officer (CFO), with great effort and against much resistance, to start looking at the data recorder after every flight. They did, and one of the first things he saw was numerous instances when they were putting the flaps down too fast while the plane was traveling too fast—a flap overspeed condition.

The flaps are the surfaces on the trailing edges of the wings that you use for takeoffs and landings. Flaps enable the plane to fly slower. When the plane is moving slower, you need less runway. However, the wing is less robust when the flaps are out, and there is a speed limit for putting down the flaps. The speed limit might be 250 knots, and it might also say that if you use the flaps above 280 knots, you have so exceeded the maximum speed limit that you may have breached the structural integrity of the wing. If the structural integrity is breached, the airplane has to be taken off the line for three whole days for a major disassembly, inspection, and reassembly—three whole days! So, by looking at flight data recorders after every flight, he noticed a bunch of maintenance events for flap overspeed. He goes to the pilots and says, first, that they will not be punished in any way for what they report and, second, asks why are they routinely putting the flaps down while the plane is going too fast? The pilots reported that air traffic controllers were bringing them in too high and too fast, and they had to do something to get rid of all that energy or they would not be able to do the approach successfully the first time. If the first approach was unsuccessful the first time, that would mean a go-around, which was more work for the controllers, more fuel burnt, angry passengers, etc. So the pilots were trying to do the right thing. It was not that they just did not like the rules. They were trying to do the job right the first time. The VP then realized that this was not a pilot problem, but rather this was a system problem. So he went to the FAA, the regulator, who also employs the controllers who bring the pilots in high and fast, and says, “You are the guys that are putting my pilots in a situation where they have to do what they should not do in order to complete the approach successfully the first time. What can we do about this to fix the problem?” So they fixed

the approaches. It turns out that many of these approaches were wonderful for DC-6s and DC-7s (piston engine propeller aircraft) but not so good for modern jets. The approaches were just out of date. Once the approaches were fixed, the maintenance event flap overspeeds, which again used to take these airplanes off the lines for three whole days, were reduced by 90 percent in less than a year! When you look at how much money was saved and the safety benefit of not having potentially compromised airplanes, this is a great example that proves that there is a huge productivity benefit to these safety programs if they are done properly.

Here is why this such a challenge. In most regulated industries, the regulator identifies the problem and tells the industry what they need to do about it. Then the industry tells the regulator they disagree with the identification of the problem and that they disagree even more with the solution proposed because it will hurt productivity. They argue that it will not fix the problem, and they resolve to fight it. The industry will litigate, and to the extent they absolutely have to comply, they will do it minimally and begrudgingly. In other words, the relationship is adversarial.

When aviation started collaborating, it was a whole different paradigm. They started thinking out of the box because of this simple arithmetic problem—a flat accident rate multiplied by twice the flight volume. They said, “We have got to do something different.” Einstein said that insanity was doing the same thing over and over again and expecting different results. Well, this was something different. This was collaborative, and by the time something exits from that kind of process, everybody is firmly on board with it. Everyone has buy-in because everyone’s considerations were taken into account when deciding what to do. Not only that, but now they promptly and willingly implement the improvements instead of fighting and litigating them. I guarantee you that when you come up with a solution in a complex system, it is probably not going to be quite right and it is going to need some tweaking. There is no way the regulatory process can tweak. This collaborative process can tweak because everyone has an ownership interest in it and they want it to work. They tweak it so the solution is more effective, more efficient, and much less likely to have unintended consequences. Again, all of that occurred in aviation without generating any new regulations.

I have never seen any other industry do this collaboration as well as aviation, at the industry level, before or since. Why has that not happened? First of all, it starts with human nature. Human nature says, “I am good, and you are not.” *I* do not need to go to the marriage counselor; *you* should go to the marriage counselor. That is human nature. That means the manufacturer is going to say that if pilots just fly them like they are supposed to, and if ground crews maintain them like they are supposed to, then there would be no problem. The airline would say that if the manufacturer just built them right and the pilots flew them right, then we would have no problem. The regulator would say that if everyone would just follow the rules, then everything would be okay. Everybody

says, “I am fine, and you are not.” That is the number one challenge.

There is an additional part—the participants may have competing interests. Labor versus management, airline versus manufacturer, etc., and all participants lack trust. After most airline crashes, the airline and the manufacturer are both defendants. They are beating each other up in court, and then we come along and ask them to play nice together. You already heard earlier today from Mike about the regulators in your industry not being welcome, about people being skeptical of why the regulator may be there, assuming the regulator is there to fish for information that can be used to levy a fine. Of course, nobody wants them there. That is why the regulator has to back off. In defense of the regulator, when they go to Congress to get more money, what is their number one metric? Look at how many times I have used the big stick. Look at how many enforcement actions I have brought. Why? Because they can measure that. They cannot measure how much they have improved safety. That is a tough one for them to measure. In our business, we can go for years without a crash, but how do you show that you improved safety? That does not have the granularity that you need, whereas the regulator can easily show how many times they have brought enforcement actions. Plus, in many cases, the regulator does not like a democracy. The statute says that the regulator is in charge, so they want to decide what happens. Well, this collaborative process is not a democracy, either. It is a rich source of information where everybody understands everybody’s interests in a way that they never did before, and that includes the regulator. This effort requires everybody to be willing, in their own enlightened self-interest, to acknowledge that the pie can be bigger if we all work together instead of following our myopic self-interest. That is the challenge of collaboration, and what it takes to make it work and achieve a positive result is trust. That kind of trust is hard to build and easy to destroy.

All of this does not just happen by itself. It happens because you have good leadership, progressive leadership, who is committed to safety. But leadership cannot say, “There must be no errors on my watch.” As soon as you say that, humans will make mistakes, and there will still be errors on your watch. In that kind of an environment, the temptation will be to sweep mistakes under the rug. The attitude cannot be no errors on my watch. Leadership has to acknowledge that mistakes will happen, which means that the real goal is actually continuous improvement. The goal is not zero defects or else more punishment—it is continuous improvement.

Leadership also has to say, “I am in this problem, too.” It is not as simple as observing that something went wrong and deducing that I need to train you guys more. Training, training, training—that is what they always used to say. Something goes wrong? Training, training, training! That is very different than admitting that the leadership are the ones who provide the resources and establish the conditions under which everyone operates. Also, if you say that personnel are the problem and the solution is simply to do more training, this is very polarizing. It causes people to think that they are

the problem. Leaders must shift to thinking that we are all in this together.

In addition, it is very important to make safety a middle management metric. If it is not and the person from the floor says that they have got a potential safety problem, middle management may be unhappy if action would interfere with their productivity goal. That is called a workaround, when people from the floor are ignored by middle management who says, “Safety is not a metric for my raise. I want productivity! Go fix it yourself.” It is crucial that leadership makes safety a middle management metric.

Another suggestion is to engage labor early because labor has got to do the work. If labor is not on board with a solution, nothing is going to happen. So engage labor early. Include everyone who has got a dog in the fight because if someone is involved in the problem, they need to be involved in the solution.

Last but not least, reporting and the information from the front line is the fuel for this process. Leadership has to facilitate the collecting of that information, its use, and make it happen. Here is what the regulator can do—demonstrate a safety commitment. That means continuous improvement and not more punishment. Emphasize the importance of “system think” and not just looking at the worker and punishing. Look at the system in which these well-intentioned, proud, and competent professionals are trying to do the right thing. Encourage and participate in “system think.” It is the regulator who decides how to protect the information that is provided, because if people are afraid that the information they provide is going to be used against them, they will not provide it. The one who ultimately decides that that information will be protected is the regulator. So the regulator has to announce policies for protecting that information and the people who provide it and then make sure that other industry participants do the same. We know that in any organization, the leaders must demonstrate commitment in order for that organization to have a safety culture. I am saying the same thing about an industry. The industry leader is the regulator, and the regulator must demonstrate that commitment in order to have a safety culture.

I would submit to you that I gave you the industry-wide example. I would submit to you that collaboration can work at any micro- or macro-level problem that you need to fix. Could this apply to you with power systems? Here is what I suggest. To me, the industry-wide example is a run. I suggest that you first crawl, then walk, then run. The crawl stage would be taking a troublesome area, something that has been nagging, something that you have tried to fix for years—this fix, that fix, nothing is working. When you have that problem that has been happening for years, there is a very good likelihood that the problem is the process (or system) and not the people. So that means it is time to fix the process. I would suggest selecting a collaborative corrective action group to look at this problem. Take everyone who has a dog in this fight, bring them together, and work on the problem in a collaborative way.

Safety culture is important not only at the individual organizational level, but also at the industry level. That is what we discovered in aviation. Just as the organization's leaders have to demonstrate commitment in order for the organization to have a safety culture, the regulator has to demonstrate commitment in order for the industry to have a safety culture. We found in aviation that if you want the safety improvement program to be sustainable, it has got to help the bottom line. And we found that collaboration is the key to making safety improvements and helping the bottom line.

Thanks for the opportunity to be here, and I look forward to the question and answer discussion. It is fascinating to me, because anytime I listen to another industry, I learn and think, "Wow, I can take that back home and apply it to my industry." I hope this will be a win-win, that you will learn from this and think about how to apply this to your context. I am already learning from it, so thank you for the opportunity to be here.

VII. GROUP DISCUSSION

Q: **[Audience Participant 1]** This question is for Michael Moon. There was an industry expert team of utility members that was formed, and they produced a report about a year ago. They had selected a number of standards that did not directly impact reliability and should therefore be removed. Where does that stand? Could you just give an update on that?

A: **[Mike Moon]** Yes, and by the way, one of those industry's experts is here with us today. We have a requirement to review standards every five years, and we contracted with five senior industry experts. Between the five, they have over 120 years of industry experience, they covered the geography of the continent, and they represented all aspects of operations and planning. There was an additional member of the team from FERC and an executive from NERC. They went through every standard. They laid out a method to assess the content, the quality, and yes, they did identify standards that are still necessary but need to be revised and a bunch to be removed. We are in the process of working through how we do that. This is a follow-up to FERC Paragraph 81, where FERC opened the door to identify the purely administrative or poor-impact requirements [11]. The Director of Standards could give you a better answer in terms of the exact status, but we are using that to inform various standards projects and prioritize, and that report is still very much being relied on. The expertise of that team was incredible.

Q: **[David Costello]** Chris Hart mentioned that while looking at accident or safety rates is difficult, what you are going for is continuous improvement—identify, measure, and improve. It is important to know what you are measuring. How do we really measure that all of the time, effort, and costs that we are putting toward these efforts—complying with mandatory standards—are improving reliability?

From the NERC state-of-reliability report and Kris Koellner's presentation, we see that the misoperation rate has been flat over the past three years. When we look at causes in the pie charts, we see general categories like settings, logic, and design. But there is another layer deeper

that we can go—why did the setting error happen? Why was the design error not caught during commissioning tests? What should we measure? How do we know we are making progress?

A: **[Kris Koellner]** In ERCOT, at the System Protection Working Group, we work really closely with one of Mark's coworkers, David Penny, at Texas RE who provides us with a wealth of information in terms of misoperation reporting metrics. We are specifically focused on that topic. Cause codes are a challenge, as you cannot make it too detailed or else you would have a million of them, and you cannot make them too high level or there is not much to learn. Fine-tuning that is a skill unto itself. I feel like the data is pretty good in terms of having something to act upon and having something to dig into.

A: **[Mark Henry]** NERC has an effort to identify risks to reliability. Misoperations is one that they have on the list. The NERC effort is going to become more a part of everything that the ERO does. We are all going to get together and look at those things. We are not going to have a lot of big, catastrophic system events. We want to avoid that, but for us to key off of that as a measure is going to be rather difficult. So we have got to identify components of risk and find some reasonable targets within that. We are at a 50 percent human error level. If we have got enough data, we can really dig in at that a bit more and identify certain activities and develop an approach to reducing those things. It depends on having input on what we believe the biggest risks are and then starting to attack those things.

A: **[Mike Moon]** The FAA has a very simple metric that is incredibly impactful—fatalities per miles flown. It is real simple. That is one metric about death. In the ERO, we have got an adequate level of reliability metrics. We have got misoperation statistics, the Generating Availability Data Systems (GADS), the Transmission Availability Data Systems (TADS), misoperations databases, cause codes, etc. One of the jobs of a good regulator should be to influence the industry. One of our metrics for the NERC staff is there will be no Category 4 or 5 events in any calendar year. If there are, we all lose 10 percent of our incentive compensation. It is difficult to clearly correlate our actions to improved reliability and safety. That is always really tough in terms of the public trust mission of a regulator. The second part to that metric is that the composite index of Category 1 through 3 events should be trending downward or flat. Our job is not to drive events to zero. That is a metaphysical impossibility. But we do want to lessen the severity of events. We are working hard to figure out what is the best metric and identify one, like the FAA has, that everyone can look at and agree is really clear.

A: **[Chris Hart]** We have so few crashes (knock on wood) that we are finding that the metric of death per flight is not granular enough, that it is telling us sort of warmer or sort of cooler when what we really want to know is 71 going to 72 degrees or 71 going to 70 degrees. That is the granularity that we are looking for, and we are still in a learning curve, collecting more data so that we can get much more granular about it. Yes, certainly, crashes are a metric, but it is a reactive

metric. It is not granular enough to know whether improvements that we are making are working. So we are struggling with that as well.

Q: **[Audience Participant 2]** Chris, in your successful process of collaboration between the parties, how do you achieve balance and avoid any one entity, such as the regulator, from getting any upper hand, which would sort of be like a hijacking of the success of NTSB to date?

A: **[Chris Hart]** That is a very good question, and that is why I am not surprised that I have not seen industry-wide collaboration in any other industry that matches aviation. It is a tough challenge to get everybody with competing interests to come together and work together in their enlightened self-interests and realize how much they can raise the water for everybody when they work together versus me against you. That is a big challenge, and I credit our success to two progressive individuals. One of the major enablers of the amazing collaborative safety process in aviation was the regulator, the head of the FAA, who believed that the best way to make an already good safety record better was to improve collaboration with industry rather than to increase enforcement. The second was the VP of Safety that I talked about who worked on getting the data read out of the flight data recorders after every flight and consolidated. So that is what we had, the fortunate coincidence of two progressive leaders (one in the industry, the other at the regulator) who came to work together, to bring people together. It was a slow process because it is a trust process and that takes a while to build.

Q: **[Audience Participant 2]** How will you maintain that? After their progressive leadership, and the trust process, which is a tremendous success that continues to build, I believe, how are you going to maintain that so that it does not drift off or regress?

A: **[Chris Hart]** My theory—and it is just my theory—is that this process and relationship is maintained because it improved productivity as well as safety. Once the industry saw improved productivity, the process achieved sustainability needed to keep going.

Q: **[Audience Participant 2]** So you think the parties just do not want to mess with the success of it? That is keeping it stable?

A: **[Chris Hart]** Yes, correct.

Q: **[Audience Participant 3]** I have a couple of questions for Chris. At the California ISO, some of the most valuable information we got from operators was on near misses. Quite frankly, you do not want events because that creates a lot of paperwork, a lot of conversations that distract you from reliability. Is there a method that you have come up with to capture near misses and to be able to share that in the industry? That is one of the things that we miss, and part of it is because we do not have the event analysis quickly like we used to, within a week with all the involved parties. Now, with the lawyers involved, we do not do that anymore.

A: **[Chris Hart]** That is a very good question, and the answer is yes, because the fuel for the CAST process is that most of the U.S. carriers now submit their flight data from

their flight data recorders to a central source, MITRE, which now has millions and millions of flights in their database. When CAST first started in the mid-1990s, tall poles in the tents were accidents, but now they have taken care of that for the most part. Now they are looking at near misses, which manifest themselves in the millions of flights in the database. That is why that data is so valuable, that is why I say it is the fuel for the process and we could not operate without that data. We managed to get that data because we obtained legislation that protects that information. If it is voluntarily provided, it is protected from being revealed in a Freedom of Information Act request. That was one of the big concerns. If I send my data to the government and the government has to respond to the Freedom of Information Act, does that mean that some newspaper reporter could show up and demand all the information on some instance and then my name is in the newspaper? That legal protection is what enabled the collection of that massive amount of data.

Q: **[Audience Participant 4]** The way we handle the near misses is that we have a safety meeting once a month, and no one has pens, pencils, or papers. Everything goes on the whiteboard, and there are no names so we look at it from buckets. We say this is because of the system failure, this is because of the resource constraint, or somebody was working too much overtime, and from those, we prioritize what we need to do on the near misses. But there is no record other than what is on the whiteboard, and we just erase that (so to speak) from the legal perspective.

Look at our industry in 2007, when we went to the mandatory standards compliance, and compare to the nuclear industry. They started in 1971, and they took almost 40 years to be where they are right now. We are only seven years into it, and we have made huge progress, especially since Gerry Cauley took over. NERC will be in Salt Lake City talking about RAI, what it is, and your internal controls. We are going in the direction we want, but there are a couple areas in which I think we are still struggling. If we have doubt, then the standard is ambiguous. Where do we go? If we call somebody and get an interpretation, that provides no guarantee that an auditor later will share the same interpretation. This is an area that I think we need to work at. Other than that, I think that my request to you, the audience, is to get involved. Go to the standard development committee meetings, because if we do not spend enough resources on the front end, then we end up spending a lot of resources at the tail end. Second is that if you look at the Institute of Nuclear Power Operations (INPO) and the Nuclear Regulatory Commission (NRC), they work very close together. This is like the Transmission Owners and Operators Forum (TOOF), now the North American Transmission Forum (NATF) run by Tom Galloway, that I think is working well. Transmission owners need to start participating. And stop complaining—we are partly responsible. Before 2007, the industry said that we were in compliance. As soon as standards became mandatory, look at the self-reported violations we filed! We lost their trust. So now we are trying to establish trust as well as work with the regulators. So you are doing a good job, Mike, and

take that back to your folks. We will work with you, learn from Chris's model, and get a better understanding of where we are. Thanks.

A: **[Mike Moon]** Regarding ambiguous standards, you can have standards that may not be perfect, but if you have well-trained auditors, they should be able to deal with that reasonably. Remember, auditing does not guarantee reliability or guarantee assurance, it provides reasonable assurance. And auditing is a profession just like engineering, just like piloting an aircraft. A good auditor should have credentials, education, experience, and learn about judgment. We are really shifting the focus, again, away from the check-the-box auditing and more to judgment. One of my favorite examples is that you can have PRC-005 maintenance systems, and you are on some pretty tight schedules. Then, all of a sudden, Hurricane Sandy happens. What do you do? You send some of your crews to help, because of mutual aid agreements, another entity get customers' power back. And then your maintenance schedule slips. Well, by the checklist, you are out of your maintenance schedule. But these are some of the other things we have to teach auditors. That judgment part is understanding that you went to do something better, to help those who were out of power, and that letting your maintenance slip had minimal risk. We have to train our auditors better. We have upgraded the auditor checklist; we have an auditor handbook; we are doing auditor training through the RAI.

Regarding the NRC and INPO, they do work very well together, but keep in mind, you also have a very homogeneous industry, if you will. Some 66 generating stations, 103 plants, and they have a different function. Their function is radiological safety and a rapid and safe shutdown of a reactor if something bad happens. That is very different than reliability. And, when you look at those nuclear generating stations, there is a very different sort of mindset. We have 1,900 very diverse entities. We have everything from the nuclear plant down to a small gas peaking plant. This is exactly why one size does not fit all. Standards have to have a level of flexibility to compensate for that diversity and allow for different system designs, configuration, and business practices. We are doing a lot of work with NATF. We are working on misoperations, CIP Version 5 transition, a 345 kV breaker alert, or a follow-up on that advisory. So we are working with them. But, just in fairness, I love all 75 members of the NATF, but all 1,900 entities that we have jurisdiction over are my favorite. But, yes, we work with NATF.

Q: **[Audience Participant 5]** Chris, this goes back to you saying that you wanted to learn something about our industry. From our industry view, a big shift that has happened is that we have replaced the days where devices tripped and there was a physical flag or target visible only if you physically went to the device to today where we can get time-synchronized data in real time back into our control centers. Large investment is happening in our utilities to make real-time decisions during hurricanes and storms, to dispatch crews, what we call situational awareness, and a lot of that has been driven by improvements in technology.

I was very interested to follow the story about the lost Malaysian Airline Flight 370. One takeaway I have from the press release was that the black box in these very expensive jetliners cannot be retrieved until you physically find the thing. Is there any discussion about fixing that and pulling data out in real time over radio or some fast communication method?

A: **[Chris Hart]** Yes, it is just a matter of time before that happens. It is a bandwidth issue right now. The technology is pretty simple, but it is a bandwidth issue. It is just a matter of time before all airplanes are going to do uplink-downlink to some central place and have real-time information so that we do not have to look for the boxes anymore. I can tell you as long ago as 1990 or so, railroads began doing that. They would uplink-downlink from the locomotive, and they started getting good at being predictive with the information. So the people in the maintenance base would look at this data, your oil pressure, your oil temperature, and that is the signature that shows that you are about to lose your oil pump. So the locomotive needs to replace the oil pump at the next maintenance station that you come to, instead of risking a dead engine in the middle of Montana. It is just a matter of time before we will have a much richer source of information, and we will not have to look for the boxes anymore. It is a bandwidth issue, with the number of planes we have today.

Q: **[Audience Participant 6]** Risk is the probability of failure on demand times the consequence. As a registered professional electrical engineer, I take the responsibility for public safety first and foremost. Death and failures that lead to injury or hazard to the public are high on my list. I am wondering, from your perspectives, is there a regulatory frenzy about the lights going out? I am not trying to minimize loss of power and the impact that it has on the economy. There is certainly an impact on personal safety, or the potential of that, but are we making more of this than necessary? As you know, there is a lot of money on the regulatory side that is going into this, and a bit of a frenzy about it.

A: **[Kris Koellner]** Something I have been thinking about lately, and discussing with the panelists, is that utilities are repairable systems. In some cases, the lights can blink and literally 15 minutes after the lights blink, it is as if that event did not happen. That is a lot different from when an airplane falls out of the sky or a locomotive goes off a track or the medical operation goes wrong. It is just something that is different about our industry.

Now the caveat is that the same error that led to a certain misoperation that is fairly innocuous (for example, a failure to reclose) could be an inherent flaw in an engineer's thinking that may lead to a failure to trip when a power line is down in a playground. You can learn from those innocuous mistakes and prevent the real impactful ones that cost you \$20 million and lead to a fatality or some sort of serious impairment.

But, it is hard to get motivated sometimes to look at all misoperations evenly because the power system sort of reboots itself in many cases. It is not like a satellite that you send off to Mars that better be right because you only get one

chance. That is not a repairable system. Transmission grids are, to some degree, repairable and recoverable.

A: **[David Costello]** At this conference a couple years ago, we had a utility executive who said that there was nobody in their boardroom that thought that installing a distribution automation system would not improve reliability or would not add another 9 in a far-out decimal place at the end of their availability measurements. But would any customers pay for that? How would they get reimbursed? That was a real dilemma that he had in his utility. He was being very frank and honest.

A: **[Audience Participant 3]** Let me share some thoughts about blackouts. I got a phone call from Homeland Security one day after the Fukushima incident. They had identified us as a sort of expert in being able to shed large blocks of load and not create civil disruption. The Japanese wanted to talk to us and were concerned about what happened to society when they had to shed loads. They were concerned about high-speed trains that would go really fast for 10 minutes, only to then sit for 4 hours at a town they chopped off when they did their load shedding. They could not even get to work and back.

To the point about blackouts and the costs, back after the California energy crisis was over, the Pentagon wanted to talk to me about the costs to society and national security risks due to base closures. What they did not realize is that the ISO did not shut anything down. The ISO would tell utilities to shut off a certain block of load. But evidently some bases were turned off and that created a national security issue. But when the discussion got to the point that you brought up about what is the cost and why do people get so excited, know that the California ISO interrupted 500 to 1,000 MW 13 different times, and we were told that had an economic cost of \$23 billion. Did I expect that? Did I have any idea about the costs? Absolutely not. But they made it perfectly clear that they did not want us to do it again. If there is a frenzy, it is because power outages have huge impact beyond money. But the amount of money is also tremendous.

Q: **[David Costello]** The aviation safety reporting system has been around since the 1970s and that provided a confidential way for people to self-report mistakes, problems, near misses, errors, things like that. For a lot of decades, aviation has been looking at data. For us, in our industry, step one is we are trying to provide a similar safe way to share data. CAST seems to be when aviation created a team of people to collaborate, to act on the data, and that is really when it started making headway in the late 1990s. We have NATF, the IEEE PSRC, NERC, etc. Do we have too many players? How do we coordinate all these different, diverse groups that have overlapping goals and missions? How do we get all these people together?

A: **[Chris Hart]** This is one of the reasons I suggest starting with a micro model instead of a macro model. To me, the industry-wide approach is the most macro you can get. I am suggesting starting with a micro model and taking some issue in a plant, for example, that is very troubling and that has been very troubling for years and you have tried fixing

this and that. Start building successes on micro models, and then it can start to grow. That's my suggestion.

A: **[Mike Moon]** With the breaker failure example, we found a problem, and we took our careful analysis to the NERC event analysis subcommittee, which is made up of stakeholders. We took it to the NERC operating committee, which also includes stakeholders, and we took it to the NERC board of trustees and discussed it with the member representatives committee, the most senior level of stakeholders that advise the board. We had a big discussion about what is the best tool to use and the options on the table at the time. We could request the transmission forum help broadcast an advisory, or we could do a recommendation and require the industry to report back to us. We decided to use other existing bodies because we thought the risk was very manageable, and we felt we had a good sense of exactly what the issue and risks were. I think we did a good job there at a micro level and can say our view of risk was very calculated. It is about trust. It is about aligning everybody's interests. And you have got to find the right organizations to work with. Again, we are very diverse. Small generators, big generators, investor-owned utilities, vertically integrated markets—it is very complex. But we are going to continue to look at ways to deal with reliability risk and get to that model. It is going to take us some time, but we are pushing for it.

Q: **[David Costello]** I will speak from a manufacturer perspective and as somebody that analyzes a lot of event data with utilities. We obviously see a lot of things we think we could point out and improve, but we cannot play at the NATF. Correct me if I am wrong, but I cannot be a member, so we are on the outside. We are not a NERC entity, so today we are on the outside as a manufacturer. We have to be invited to the table to cooperate. You know, one of the reasons that we are doing this session, quite frankly, is to start these relationships.

A: **[Audience Participant 1]** I think we have got a good opportunity and a good setup right now. IEEE has its purpose, NATF has its purpose, and so does NERC. The NATF, from our standpoint, and we participate a lot, is involved with a lot of the best practices and helping with misoperations. We had a special protection system (SPS) misoperation, and we had to work through the NERC event analysis team to provide a report of that event. But, prior to that, being a member of the NATF gave us access to a challenge board. The challenge board is all the member utilities, and they look at our event report prior to it going to NERC. We may have blinders on as we look at this event, and this peer review allows the other utilities to ask us questions and we provide a better report to NERC. For those 75 or so members of NATF, those utilities cover a big part of the grid in the United States, and they are looking at best practices, doing all the right things, and it gives a big voice if we want to talk about standards, whether that is at IEEE or NERC. It is a really good setup, I think, to give one utility other brothers and sisters to help them out and get through the process of looking at each standard. When you ask if we have too many people involved, really I think it creates less because you have a big membership with one voice.

Q: **[David Costello]** A follow-up question for you. If I, as an industry engineer who happens to work at a manufacturer, who also happens to have an engineering services or consulting division, wanted to gain access to all of those best practices that NATF members are producing, do I have a way to access that information?

A: **[Audience Participant 1]** No, you do not. It is a confidential group. There is certain information, if it is system protection related, for instance, we can work through and maybe provide some information back to the vendor. But, if you are working with a utility and you think you need to share something, and that utility is a member of NATF, they should be sharing it back to their best practices group. So, it is really a utility membership.

Q: **[David Costello]** So at the heart of that, there is a real big concern about confidentiality and sharing information. I have got a question for the two attorneys on the panel. Does it make sense to you to have the event analysis, the lessons learned, and the information-sharing group be the same group that enforces, audits, and ensures compliance? I am reminded here, Chris, of the aviation reporting system. Correct me if I am wrong, but that information went to the National Aeronautics and Space Administration (NASA) and not the FAA, as an independent, third-party broker of the data. Was that needed? Why was that done? In your opinion, does that really ensure the free flow of information?

A: **[Chris Hart]** Regarding your question about who did the data go to, it did not go to the FAA because nobody trusted the FAA to have it. Nobody trusted that the FAA, having that data, would not want to enforce with it. So that is why they had to have an independent third party. This program was started in the mid-1970s, and when it originally started, data was going to be sent to the FAA but nobody came to the party. So they decided to do something different. That is why it went to NASA, but when the data goes to NASA, it gets de-identified, and that was done to eliminate the problem of people going to NASA with subpoenas to show all of the information. As soon as NASA got the data, it is amalgamated data and not identifiable to any source.

A: **[Marty Golden]** I think any information sharing with the regulatory agency obviously does not make sense unless it is coupled with some sort of defense, safe harbor, that we have talked about that would actually encourage people to do that sharing. Without that, it would make more sense to have the data reside with a third party. Whether it is with a third party or the agency, there still has to be that protection that, for your industry, does not exist now. That really is the first step. How you structure it once the protection is in place from my perspective is not too important. It is just that without the protection, there is a disincentive to share in the first place. I think you have that right now. Look at the answer you just got to your question, to something that would obviously be very relevant to what a manufacturer is doing.

A: **[Chris Hart]** Speaking of incentive, I forgot to mention that the incentive in the aviation reporting system was that if you submit a report within 10 days of an event, then the FAA, even if they find out about the event by some other source,

cannot go after you for that event. That was the incentive provided for people to submit that information into the system. Even when it confidentially went to a third party, NASA, the industry felt that it needed an incentive for people to want to participate.

Q: **[David Costello]** Was that protection from a law passed by Congress or a regulatory action by the FAA?

A: **[Chris Hart]** It was statutory.

Q: **[Audience Participant 7]** Renewables are coming online a lot quicker, and they behave totally different than the copper that we used for generations. There are some things we do not know, but how do we share information with each other to try to learn more about the system and educate each other if we have to be careful about how we write our emails and correspond to one another?

A: **[Marty Golden]** Without being specific to that example, as I said earlier, the whole thing about emails is that we have turned this into a form of conversation that replaced what used to be done orally and what used to be done with no concern about the record being created. But emails create records now. If it is a family or friendship thing, it makes sense, but for people in the industry to be communicating at that informal of a level about things that they are doing with their jobs and about things that, potentially, they are going to have to be explaining later to somebody, then that is not in their best interest. It is just that people are not thinking about the business environment that we are living in today. With every email that pertains to things that take place in the workplace that they circulate around to management and coworkers, people need to think about who it is being sent to and what is being said before you hit send.

Q: **[Audience Participant 7]** We pride ourselves in returning our customers' questions as quickly as possible, but what you are saying is to think six, or seven, or eight times, before replying. Should I now degrade my customer service, think about this for 24 hours, to allow time to think about all the legal aspects? Do I need to put a large, legal disclaimer on my email?

A: **[Marty Golden]** The legal disclaimer is really not going to do you any good. People think it does, but it does not. I do not think you need to wait 24 hours to respond, but the reality is (and we have all done it; I have done it), you hit send and then think, "I wish I had made some changes before I sent that." But it is too late at that point. The other thing is just the culture of emails. In this era of social media, this era of immediacy of communication, even when we are not speaking with each other face to face, we have developed some sloppy habits. All of this may interfere somewhat with what you believe is your first priority of customer service, but I think the reality is that you have got to think of both sides of it, at least somewhat. Just change the culture a bit. It does not mean give less customer service, but ask David about all of the customer service emails we had to address in the lawsuits that I dealt with for SEL. It was a huge headache.

Q: **[Audience Participant 7]** Are you saying to make that answer as vague as possible?

A: **[Marty Golden]** Well, let me ask you this. Why not just pick up the phone and talk to your customer directly? Just for example, if you are transmitting drawings, or settings, or something along those lines, then obviously that is going to have to be sent in an email format. I am referring to the more traditional communications that all of us now do by emails. I do it myself. It is wonderful and a great convenience, but there needs to be a little thinking about the fact that, instead of what you and I are doing right now conversing, that email is getting stored on our server, it is not going anywhere, and it may have to be explained in the next three or four years to somebody who really does not care what it means. They only care what kind of a case they can make out of it. It is a culture shift. It does not mean you stop providing customer service.

A: **[Chris Hart]** A real-world test that you often hear about in the federal government is if you would not want this email printed on the front page of the *Washington Post*, then do not send it.

Q: **[Audience Participant 7]** Some want an explanation. Do you forward them a hypothesis? What is possible? If you put it on paper, you make a sketch to show someone how it works. So what you are really saying is do not do that. Just pick up the phone and talk to them.

A: **[Marty Golden]** No. That is not what I am saying. What I am saying is that you have to do your job. The other side of this is you cannot be paralyzed in doing your job by the fear of potential liability of all this stuff. But you also cannot be at that other extreme of not giving any thought to this at all. This means, as I mentioned earlier, to consider things like reply to all, especially if there are people that do not need to be hearing that communication, then delete those names from the email before you send your reply. And, just in general, think about whether you need to provide those specific details in this particular response. Does your reply go beyond the question that was asked? Is the reply opening the door to some more unpleasantness that you are going to have to address down the road, potentially? Once you actually have to do that a couple of times, you will get it.

Q: **[David Costello]** I have a question for the group and maybe Kris can help me out a bit because you described how your compliance efforts are set up inside LCRA. You have managers and SMEs, and you divided the work out. I think you said you have three dedicated compliance people. Is that common? We have a lot of people that are here in the audience. I would like to hear from you, too. Is Kris very unique? Is his company pretty close to what your companies do? Does anybody want to share a little bit about how they are organized and how their compliance efforts operate?

A: **[Audience Participant 8]** We are very similar to that. We have what we call a compliance committee. We have two people that actually work in compliance. Then we have a substation guy, a transmission guy, a planning guy; so we kind of have some managers that are responsible for our TO, TP, etc., registrations. Then, underlying that, we have SMEs for protection stuff, planning stuff, whatever. That is how we are set up and that seems to have worked pretty well for us for the last two or three audits. We do not have one person trying to

be responsible for a myriad of things. That has been stated—no one person can be an SME for all of that.

A: **[Audience Participant 4]** We are looking at different models right now and are in the process of changing. We looked at the PJM model on the compliance as well as reliability standards sides and how they are structured. We have an independent compliance group, which has its own vice president level; then we have two sections, internal plus external. Once a standard is approved by FERC, then we get into the implementation process. We decide who is going to be the owner of the standard, create new positions, and fill those positions. We call them the RSO, reliability standard owner. When it comes to sending the information, the RSO is going to be coordinating everything, providing the comments, and looking at the standard development process. I think our model is similar, but we have defined very clearly who is responsible, and we have metrics of the name of the organization that is there and not the person.

Q: **[David Costello]** Kris, I assume you fill out a timesheet to account for your hours. We are hearing a lot about spending a great deal of time managing compliance. So I am curious. Are you tracking the cost or the hours spent on compliance?

A: **[Kris Koellner]** We do not break it out to that level of detail. That would be interesting to see. For us, it is embedded in the transmission rate that we recover.

A: **[Audience Participant 4]** We established a work order for the last three years to track this. Not including NERC CIP, our costs are between \$10 and \$11 million. Our jaw dropped when we looked at how much time, money, and resources we spend. If you do not track, then you do not know how much time and money is being spent.

Q: **[David Costello]** Did you say \$11 million? Over what time period? And this does not include CIP?

A: **[Audience Participant 4]** Correct, \$11 million. Over one year. If you look, \$10 to \$11 million, most of the people are not still charging the right time. If you collected all, my gut feeling is that it would be around \$14 million. CIP might be two to three times as much.

Q: **[David Costello]** This brings us back full circle. We are all concerned about reliability. Are we spending the time, money, and efforts in the right place? Mark and Mike, you also spoke to adding a little judgment into the auditing process and allowing a little leeway on time. Is that becoming a bigger part of what you want to do?

A: **[Mike Moon]** Yes, absolutely. One of the things about auditing is that it takes judgment. It is its own profession, and it has some art to it. Every single entity that asks for an extension on an event analysis report or compliance self-assessment gets it. Every single entity is allowed whatever time they need as long as they are working in good faith and keeping us updated. When they do a good job in a collaborative way, they are going to get credit from us, and we see that as a reduced risk. One of the immediate benefits that comes through this type of collaboration, good event analysis, and compliance self-assessment is your risk is seen as reduced, your compliance monitoring will be reduced, and nobody else can give that to you but us. So again, you have

got to work with us. We want to work with you. We want to give you credit, and we want to give you the time you need to do good analysis.

A: **[Mark Henry]** I would just add that we have had a similar experience. We have had times when extensions have been mandated just by circumstances. It is not a heartless matter. There are times, too, that you may have something that carries through that interferes with our enforcement process but you end up with a \$0 penalty. We try to work within the situation we have. Again, there are 1,900 entities involved in this, of all kinds and types, so we have to consider that. The risk to reliability can vary tremendously, as well as impact, so that is something we consider. I would add that working with lawyers in the regulatory space is a challenge that all of us have learned to deal with, as well, as we go through these processes.

Q: **[David Costello]** So, as we get to the end of our session, I would like you all to take a few moments and share some thoughts about what you have heard today and close with some final remarks.

A: **[Kris Koellner]** I think, for me, it just comes down to priorities and knowing that you have got a finite amount of resources. We would all have super compliance if we would double our staff in this room, but that is not going to happen. You really have to decide on the priorities, and that is the feedback I would like from NERC and Texas RE. It is all important work, but what is the most important? How do we manage that? That is what I keep coming back to over and over.

A: **[Mike Moon]** The topic of the panel was reinventing the relationship with the regulator, and I am here to tell you that the preponderance of that responsibility rests with us. We recognize that, and we are working hard to improve things. And I think we have various examples of that improvement in action. We want to work with you. Keep working with us. We may not get to this exact same place as the NTSB and the FAA. We might not take the exact same road, but that is the idea that we are striving for as well. Thank you.

A: **[Mark Henry]** There are changes that are already under way. We recognize the need for some of this. Responsibility has been taken to do that. It is sometimes a challenge for us to work with the federal body that oversees us, as well as our state commission. Generally, they seem to be willing to listen. They are subject occasionally to what I call major influences. But, if we continue to work through this and demonstrate the kind of good performance that we have done for many years, I think that we will prevail in this.

A: **[Marty Golden]** The safe harbor, legislative, or regulatory changes that we have talked about are, at best, a long way off. It may never happen, and they will be fought against like dogs by the plaintiff's bar, by consumer groups, and other political interest groups. Until then, do what you have to do, but be smart. Understand the litigious environment in which we all live now.

A: **[Chris Hart]** I agree with Marty on that point entirely, and that is why I like the way he ended his talk with what he called "smart morality." That is actually what the airline

industry did because there is no protection in the airline industry from these very same problems that he is talking about. This information is not protected from disclosure and civil litigation at all, but they are still doing it because they engaged in that "smart morality." Kudos to them for doing that because that was a tough challenge for a lot of entities to make that decision. I guarantee that a lot of their lawyers did not like it.

Collaboration has demonstrated to be hugely powerful and successful, and it is very important if the example on which you are collaborating has a regulatory piece to it. It is very important that the regulator participates in that collaboration process as well.

Spurred on by the great presentations in our panel and the probing questions from the attendees, I have been pondering why (over the objection of many of their attorneys) so many members in the U.S. aviation industry decided to pursue various information collection and sharing policies to improve safety. I believe it is because they decided, along the lines of Marty's suggestions, that it is more important to stop crashes than to worry about litigation. That may reveal one difference between our industries that causes one size possibly not to fit all—that our mishaps are generally more likely to directly cause injury and death than your mishaps.

A: **[David Costello]** There is not a person in this room who wants the reliability of the power system to suffer. There is not a person in this room that wishes that our regulatory environment could just be a little more contentious. We did not have any illusions that we were going to solve every aspect of this problem today. We wanted to move the needle a little bit in the right direction, and I appreciate everybody being here to do that. I think that we accomplished a lot.

Part of that is acknowledging that we have to have all of the players sitting at the table to talk about a problem. We cannot get anywhere unless everybody is invited. I am reminded of Robert Bryce, a keynote speaker at our first conference. Someone asked him to define his energy policy, to which he responded, "I like cold beer and air conditioning." So maybe we can start on what we agree with—I like that. I like highly reliable, safe power systems at the lowest possible cost. I like a clean environment. I think regulation is not going away. We know that. Fining somebody for self-reporting or for minor infractions—I think we are all on board with those not being ways to dramatically improve power system reliability.

I think it is important to wrap up on a very positive note. There are, to borrow from Chris' presentation, in our industry, too, a lot of good people trying to do the right thing. I would encourage you, if you leave with just one action item, to get engaged. NERC is not a bear that lives in the woods that comes out and mauls you every once in a while. We are a part of this. Get engaged and help improve this together. It is too easy to lob criticisms from the cheap seats of the arena—get down on the floor and play a little bit. I want to thank our panelists—Kris, Mike, Mark, Marty, and Chris. Thank you very much for sharing your time and talents.

VIII. EPILOGUE

In August 2014, based on lessons learned through this panel and dialogue, NERC involved a protective relay manufacturer for the first time in the conversation with a registered entity regarding a self-reported event, analysis, and cause-coding. Learning from the aviation model and CAST, this represents a great first step in improving information sharing and focusing on our mission—improved reliability.

IX. GLOSSARY OF TERMS

| | |
|-------|---|
| AC | Alternating current |
| BES | Bulk electric system |
| CAST | Commercial Aviation Safety Team |
| CEO | Chief executive officer |
| CFO | Chief financial officer |
| CIP | Critical infrastructure protection |
| CT | Current transformer |
| CYA | Cover your [butt] |
| DAWG | Disturbance Analysis Working Group |
| DC | Direct current |
| DOE | Department of Energy |
| EMP | Electromagnetic pulse |
| ERCOT | Electric Reliability Council of Texas |
| ERO | Electric reliability organization |
| FAA | Federal Aviation Administration |
| FAC | Facilities design, connections, and maintenance |
| FBI | Federal Bureau of Investigation |
| FERC | Federal Energy Regulatory Commission |
| FFT | Find, fix, and track |
| FPL | Florida Power and Light |
| GADS | Generating Availability Data System |
| GMD | Geomagnetic disturbance |
| IEEE | Institute of Electrical and Electronics Engineers |
| INPO | Institute of Nuclear Power Operations |
| ISO | Independent system operator |
| LCRA | Lower Colorado River Authority |
| MSHA | Mine Safety and Health Administration |
| NAFT | North American Transmission Forum |
| NASA | National Aeronautics and Space Administration |
| NERC | North American Electric Reliability Corporation |
| NOP | Notice of penalty |
| NRC | Nuclear Regulatory Commission |
| NTSB | National Transportation Safety Board |
| OSHA | Occupational Safety and Health Administration |
| PRC | Protection and control |
| PSRC | Power System Relaying Committee |
| PUCT | Public Utility Commission of Texas |

| | |
|----------|--|
| PV | Potential violation |
| RAI | Reliability assurance initiative |
| RAS | Remedial action scheme |
| RSAW | Reliability standard audit worksheet |
| RSO | Reliability standard owner |
| SERC | SERC Reliability Corporation |
| SME | Subject matter expert |
| SOL | System operating limit |
| SPP RE | Southwest Power Pool Regional Entity |
| SPS | Special protection system |
| SRP | Salt River Project |
| TADS | Transmission Availability Data System |
| Texas RE | Texas Reliability Entity, Inc. |
| TO | Transmission owner |
| TOOF | Transmission Owners and Operators Forum |
| TOP | Transmission operator |
| TP | Transmission planner |
| TPL | Transmission planning |
| VP | Vice president |
| WECC | Western Electricity Coordinating Council |

X. ACKNOWLEDGMENTS

I wish to express my sincere gratitude and admiration for Kristian Koellner, Michael Moon, Mark Henry, Martin Golden, and Christopher Hart. Their contributions to the Modern Solutions Power Systems Conference, their willingness to further share that discussion through this technical paper, and their hard work and efforts to improve our industry are very much appreciated.

XI. REFERENCES

- [1] North American Electric Reliability Corporation, *Reliability Standards for the Bulk Electric Systems of North America*, September 2014. Available: <http://www.nerc.com>.
- [2] Texas Reliability Entity, “2013 Assessment of Reliability Performance: Performance Indicators Update, First Quarter 2014,” April 2014. Available: <http://www.texasre.org>.
- [3] Florida Power & Light, “FPL Announces Agreement With Federal Energy Regulatory Commission,” October 2009. Available: <http://www.fpl.com>.
- [4] Federal Energy Regulatory Commission, “FERC Approves First Settlement in 2011 Southwest Blackout Case,” July 2014. Available: <http://www.ferc.gov>.
- [5] Federal Energy Regulatory Commission, “FERC Approves Second Settlement in 2011 Southwest Blackout Case,” August 2014. Available: <http://www.ferc.gov>.
- [6] Public Utility Commission of Texas CREZ Transmission Program Information Center, “PUCT – CREZ Home Page.” Available: <http://www.texascrezprojects.com>.
- [7] United States Department of Labor, Mine Safety and Health Administration, “Report of Investigation: Surface Metal Mine (Alumina) – Nonfatal Exploding Vessels Accident,” ID No. 16-00352, July 1999. Available: <http://www.msha.gov/disasterhistory/gramercy/report/reportdept.htm#concl>.

- [8] *Bredice v. Doctors Hospital Inc.*, United States District Court, District of Columbia, March 11, 1970.
- [9] National Transportation Safety Board, "Loss of Thrust in Both Engines After Encountering a Flock of Birds and Subsequent Ditching on the Hudson River, US Airways Flight 1549," Accident Report NTSB/AAR-10/03, May 2010. Available: <http://www.ntsb.gov>.
- [10] Institute of Medicine, "To Err Is Human: Building a Safer Health System," November 1999. Available: <http://www.iom.edu>.
- [11] North American Electric Reliability Corporation, "Guidance for Compliance Monitoring and Enforcement Pending Retirement of Standards and Requirements Pursuant to Paragraph 81," April 2013. Available: <http://www.nerc.com>.

XII. BIOGRAPHIES

David Costello graduated from Texas A&M University in 1991 with a B.S. in electrical engineering. He worked as a system protection engineer at Central Power and Light and Central and Southwest Services in Texas and Oklahoma and served on the System Protection Working Group for ERCOT. In 1996, David joined Schweitzer Engineering Laboratories, Inc. as a field application engineer and later served as a regional service manager and senior application engineer. He presently holds the title of technical support director and works in Fair Oaks Ranch, Texas. David has authored more than 30 technical papers and 25 application guides. He was honored to receive the 2008 Walter A. Elmore Best Paper Award from the Georgia Institute of Technology Protective Relaying Conference and the 2013 Engineer of the Year Award from the Central Texas section of the IEEE Power and Energy Society. He is a senior member of IEEE, a registered Professional Engineer in Texas, and a member of the planning committee for the Conference for Protective Relay Engineers at Texas A&M University.

Kristian "Kris" Koellner supervises the System Protection Department at the Lower Colorado River Authority (LCRA) in Austin, Texas. Throughout his career, Kris has worked in the areas of distribution planning, power quality, and most recently, system protection. Kris graduated with a B.S.E. degree in electrical engineering from Arizona State University, and prior to joining LCRA, he worked in a variety of roles at Salt River Project. He is registered as a Professional Engineer in the state of Texas. Kris served as the 2012 chair of the ERCOT System Protection Working Group (SPWG) and presently serves as the chair of the ERCOT Synchrophasor Task Force (STF).

Michael "Mike" Moon is currently the senior director of Regional Entity coordination at North American Electric Reliability Corporation (NERC), reporting to the president and chief executive officer to support strategic planning, leadership, and oversight for the development of NERC's collaboration and oversight model. Previously, Mike was the senior director of reliability risk management, the department that maintains bulk power system situational awareness, conducts event analysis, and supports training development for NERC, the Regional Entities, and the industry. In this capacity, he oversaw the rapid increase in analysis of events and cause coding to support identification of reliability risks. Mike also provided executive oversight to the NERC stakeholder Operating Committee from 2010 until early 2014. Mike joined NERC in June 2009 as the director of compliance operations and interfaces. During this time, he initiated concepts and discussions on a risk-based approach to audit planning and entity assessment and to move away from the zero-defect approach to compliance. Mike also was in charge of outreach to the NERC stakeholder Compliance and Certification Committee, the industry trade associations, and the forums. Prior to arriving at NERC, Mike served 26 years in the United States Army as an engineer. He served in a variety of command and staff positions. Significant positions included command of the 37th Engineer Battalion, which he led during the initiation of Operation Iraqi Freedom in 2003, attached to the 101st Airborne Division. Mike also served as the director of electrical sector reconstruction in Iraq from 2007 to 2008 and was responsible for the \$4.3 billion sector reconstruction program and the generation, transmission, distribution, capacity development and operations, maintenance, and sustainment. Mike also served as the United States European Command Infrastructure Engineer from 2003 to 2005 and was responsible for the \$1 billion in military construction and the sustainment, restoration, and modernization program for over 500 installations in the command's 94-country footprint. Mike ended his military career as the director of infrastructure rehabilitation at the United States Army War College in 2009. Mike has a master's degree in national security studies from the United States

Army War College and a bachelor's degree in applied mathematics from Longwood University.

Mark Henry currently directs the reliability assessment and performance analysis programs at the Texas Reliability Entity, Inc. These programs review system disturbances, outages, and other events as well as report on long-term and seasonal adequacy of the bulk power system within the Electric Reliability Council of Texas (ERCOT), one of eight regions of the North American Electric Reliability Corporation (NERC). The programs aim to share information, improve practices, and understand risks to support reliable power systems. Prior to this role, Mark developed pilot programs in ERCOT that later became the basis for formal compliance monitoring and enforcement programs, and he contributed to electric power standards development. Mark served in several generation and transmission-related assignments at the Lower Colorado River Authority early in his career. Mark holds a B.S.E.E. from the University of Texas at Austin, and he is a Certified Energy Manager and registered Professional Engineer in Texas.

Martin "Marty" Golden is a partner and an attorney at Keogh, Cox, & Wilson, Ltd. Marty received a B.A. degree in English literature from Louisiana State University (LSU) in 1981, and following his graduation from LSU's Paul M. Hebert Law Center in 1984, he served as a law clerk for the Honorable James L. Dennis, Louisiana Supreme Court, from 1984 to 1985. He has been engaged in the practice of casualty defense litigation for his entire career, emphasizing all lines of insurance defense, insurance coverage, bad faith, product liability, legal malpractice, medical malpractice, and worker's compensation. He is a member of the Louisiana State Bar Association, Baton Rouge Bar Association, Louisiana Association of Defense Counsel, and Defense Research Institute, and he is rated AV by Martindale-Hubbell. He has practiced in all Federal District Courts in Louisiana, the United States Fifth Circuit Court of Appeals, and Louisiana District Courts and Courts of Appeals throughout the state of Louisiana.

Christopher "Chris" Hart is the acting Chairman of the National Transportation Safety Board (NTSB), having been nominated by President Barack Obama. The NTSB investigates major transportation accidents in all modes of transportation, determines probable cause, and makes recommendations in an effort to prevent recurrences. He was previously a member of the NTSB in 1990, having been nominated by President George H. W. Bush. Mr. Hart's previous positions have included deputy director for Air Traffic Safety Oversight at the Federal Aviation Administration, assistant administrator for the Office of System Safety at the Federal Aviation Administration, deputy administrator for the National Highway Traffic Safety Administration (NHTSA), deputy assistant general counsel to the Department of Transportation, managing partner of Hart & Chavers (a Washington, D.C., law firm), and attorney with the Air Transport Association. Mr. Hart has a law degree from Harvard Law School and a master's degree (magna cum laude) in aerospace engineering from Princeton University. He is a member of the District of Columbia Bar and the Lawyer-Pilots Bar Association, and he is a pilot with commercial, multiengine, and instrument ratings.