Compliance Program Documents as a Roadmap to Process Maturity

By Bryan Rushing, Quanta Technology and Bobbi Welch, Arizona Public Service

Whether your organization is new to the compliance arena as a dispersed generating resource or has a track record of experience and is seeking to move to the next level as a self-reporting entity, a key pillar in any successful compliance program is a sufficiently developed, detailed and approved Compliance Program document.

The Compliance Program document can be expanded or contracted to serve the relative size, sophistication and commensurate risk level of each reliability entity, and serves as a roadmap for the organization and staff. Employees with direct or indirect compliance responsibilities can use the roadmap to understand the company’s overarching goals and expectations and use the program document as a guide for their departmental and individual tasks.

Documentation Development & Review
Quanta Technology has worked collaboratively with subject matter experts from Independent Power Producers (IPPs), utilities and other entities to develop and/or review electronic versions of relevant program documents and work jointly with those companies to ensure a common understanding.

Continued on Page 3

Inside This Issue:

Compliance Program Documents as a Roadmap to Process Maturity ........................................ Page 1
Letter from the President ......................................................... Page 2
The Evolution of NERC CIP Rules & Staying Ahead of the Game ................................................. Page 4
NERC Addresses Physical Security with CIP-014-1 Standard .................................................. Page 7
Planning & Operational Requirements for Geomagnetic Disturbance ........................................ Page 8
International Spotlight .............................................................. Page 9
Dear Colleagues,

As the electrical power system continues to be more complex, it is of utmost importance to address electric power system reliability as one of the most important objectives in our industry today.

Under the best of operational circumstances, this is a formidable task, but add to that threats to critical infrastructure, physical and cyber security threats, changing weather patterns including events such as hurricanes, tornados and geomagnetic disturbances, it is essential to have a robust vulnerability management plan including risk assessment, probability analysis, grid hardening and response planning.

Multiple layers of regulatory oversight are also in place to address the above. In the U.S., the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC) provide regulatory guidelines, mandates and standards that require electrical utilities to spend significant resources and efforts to comply. It is important to develop strategies and plans to efficiently address those requirements in conjunction with vulnerability management plans.

This issue of our newsletter focuses on regulatory compliance topics. We share our experiences about how to:

- Develop and implement a successful compliance documentation roadmap that includes best practices, ease of execution, program scope and Reliability Assurance Initiative attributes.
- Navigate the evolution of NERC CIP Version 3 to Version 5 and the comprehensive requirements for physical and cyber security protection.
- Address the new CIP-014-1 physical security standards for stations, substations and primary control centers.
- Plan for the best outcome if 5,000 MW suddenly came through your system due to Geomagnetic Disturbance (GMD) from a sudden solar storm.

Sincerely,

Damir Novosel and the Quanta Technology Team

Recent Quanta Technology Presentations & Publications

"Best Practices Guide to Utility Communications Platform Deployment in System Automation" by D. Boroughs with CEATI -- Canadian Utilities Information & Communications Technology Conference, September 23, Ottawa, Canada


"Investigation & Correction of Phase Shift Delays in Power Hardware in Loop Real-Time Digital Simulation Testing of Power Electronic Converters" by M. Davari and F. Katiraei -- Grid of the Future Symposium, October 11-13, Chicago, IL

"Intelligent Volt/VAR Control Algorithm for Active Power Distribution System to Maximize the Energy Savings" by R. Anilkumar, et. al. -- IEEE-IAS Industrial Automation and Control, October 18-22, Dallas, TX

"Smart Asset Management for Smart Utilities" by S. Craig -- T&D Conference, Asset Management Practices for Electric Utilities: Current State & Lessons Learned, October 20-21, Los Angeles, CA

"Catching Falling Conductors in Midair -- Detecting and Tripping Broken Distribution Circuit Conductors at Protection Speeds" by E. Udren, et. al. -- Western Protective Relay Conference, October 20-22, Spokane, WA

"Transmission Line Automated Relay Coordination Checking" by S. Alaeddfini (Quanta Technology) and G. Sarkinen, G. Kauer, P. (Xcel Energy) -- Minnesota Power Systems Conference, November 10-12, Saint Paul, MN


"Transmission Automation Strategies Challenges & Opportunities in a Changing Landscape" by V. Madani, D. Novosel, et. al. -- IEEE Transactions on Smart Grid
Our roadmap for document evaluation will drive towards the following attributes:

<table>
<thead>
<tr>
<th>Best Practices</th>
<th>Ease of Execution</th>
<th>Program Scope</th>
<th>Reliability Assurance</th>
</tr>
</thead>
</table>

The review uses an industry-accepted process maturation model, slightly modified by Quanta Technology to take into account the rapid implementation of the NERC Compliance requirements over the last 10 years. The process maturation model used as the baseline has four steps. The model below shows the four phases, along with key aspects that should be implemented at the associated maturity level and an example of the tests Quanta Technology utilizes to perform maturity assessments.

### Process Maturity Levels

#### Startup
- Mix of Ad-Hoc & Formal Processes
- Training
- Documentation identified & established

#### Repeatable & Defined
- All Processes Defined & Documented
- All Staff Trained
- Compliance Tools identified & being implemented
- Organizational components established (e.g., Swimlanes)
- Process metrics being defined

#### Managed
- Well understood by organization
- Transparent
- Accountability well understood
- All compliance tools implemented
- Dashboard implemented with well understood metrics
- Documentation organized and accessible

#### Optimized
- Continual process improvement plan identified and implemented
- Regular review by senior management
- Processes reasonably optimized taking into level of risk, cost & staff time impacts

The following general program attributes should also be considered:

- **Auditable:** Does the program allow demonstration to management, auditors (internal & external), and regulators that the organization is in compliance with applicable standards?
- **Manageable:** Is the program as easy to use and maintain as possible? This encourages employees to follow the compliance program processes & procedures (ensuring compliance) and to maintain records needed for audit trail.
- **Sustainable:** Is the program flexible to allow adding new standards as developed by the ERO and RRO(s) and to adjust processes when necessary?
- **Cost effective:** Are the costs to implement and manage the program appropriate to the organization? A paper-based filing system may be sufficient for some small organizations, while comprehensive document management may be necessary for others.
- **Traceable:** Is the recordkeeping component of the program traceable in that time-based records are linked to the applicable standard in that point in time?

For more information about this article and Quanta Technology's policy/procedure development, risk assessment, audit preparation and mock audits, root cause analysis and other compliance services, please contact Bryan Rushing at (919)334-3021 or brushing@quanta-technology.com.
The Evolution of NERC CIP Rules & Staying Ahead of the Game
By Bryan Rushing, Quanta Technology

Over the last decade, the electric utility industry has been tasked with the implementation and compliance of several new sets of rules that encompass the Critical Infrastructure Protection (CIP) reliability standards. These standards provide a comprehensive set of requirements that address both the physical and cyber security protection of the bulk electric system.

The two most recent sets of cyber security requirements are: 1) the currently effective CIP Version 3 standard, which includes requirements in nine broad protective areas, and 2) the more recent FERC-approved CIP Version 5 standard, which now includes requirements in a newly organized set of eleven areas of protection (see their requirements in the table below). These requirements are intended to address the protection of the electric system from cyber threats and ensure that the system has minimized risks of failure due to cyber-related vulnerabilities or attacks.

In addition to cyber security standards, the CIP standards include CIP-001 (Sabotage Reporting) and CIP-014 (Physical Security of Substations). This article addresses the NERC CIP cybersecurity requirements.

In CIP Version 3, utilities are required to maintain a list of all their critical cyber assets located within and outside of their control centers (including at least one year of auditable information). Interestingly, only assets that were determined to be critical assets by their owner/operators are required to comply with these requirements, resulting in many facilities having no compliance obligations for protective requirements under the CIP cyber security standards.

As we move to CIP Version 5, the biggest change will be the introduction of the tiered impact rating system that classifies Bulk Electric System (BES) cyber systems into one of three categories (High, Medium or Low) based upon the impact characteristics of the facility that it supports. This approach results in all cyber assets that could impact the operation of BES facilities being in scope for the CIP requirements.

While moving from CIP Version 3 to CIP Version 5 is a significant step forward in helping to protect us from cyber security threats that seek to disrupt the reliable operation of our vital electric system, there are significant implications to both generators and utilities from the changes. For example, utilities that did not previously have facilities in compliance with the protective requirements of CIP Version 3 will now have facilities that must implement the protective requirements of CIP Version 5. All BES-responsible entities have to comply with the standards and implement CIP-002 at a minimum. However, only those that have qualified facilities under CIP-002 have to comply with CIP-003 onwards.

In several recent engagements, Quanta Technology has supported clients in planning for compliance with CIP Version 5 obligations, including critical cyber system assessment support, and assistance with the development of cyber security processes, procedures and policies. We have provided a description of our general approach to each of these efforts below.

CIP Version 5 – Critical Cyber System Assessment

The natural starting point for a CIP Version 5 cyber system assessment is a review of any existing Risk-Based Asset Methodology (RBAM) and associated processes and tools to determine any gaps associated with implementing the newly proposed NERC CIP-002-5. To do this, it is recommended to use the existing methodology as a baseline for comparison and the expertise of our Regulatory & Compliance team’s CIP Version 3 standards knowledge to identify additional areas,
Evolution of NERC CIP  Continued from page 4

assets and systems that will require evaluation and implementation to meet the CIP Version 5 requirements.

Additionally, review of the CIP-002 Version 3 methodology to identify any needed improvements in the identification and/or evaluation of relevant assets is recommended. The objective is to identify a list of action items and recommendations that are required in order to improve the utility’s existing tools and/or create new processes and tools that will satisfy the new NERC CIP Version 5 requirements.

The next step in the cyber assessment is to use the evaluation to develop processes and documentation to successfully demonstrate compliance with the future NERC CIP-002-5 requirements. The documentation and processes will list, categorize and prioritize the BES cyber systems per CIP-002-5, R1 and BES Cyber Asset Identification.

Finally, facilitated discussions must occur with the appropriate parties to collectively review and discuss the newly developed processes and tools intended to identify and categorize BES cyber systems so that the owners have sufficient information to populate and evaluate the in-scope cyber systems. The end result is to have a final set of BES cyber systems that are appropriately categorized as High, Medium or Low for application of cyber controls per the NERC Version 5 CIP-003 through CIP-011 standards.

CIP Version 5 - Cyber Security Processes, Procedures & Policies Development

Assisting in the development of cyber security processes, procedures and policies is approached in two phases. Phase 1 focuses on an assessment of the existing processes, procedures and policies, while Phase 2 focuses on the development of new cyber security processes, procedures and policies to comply with the approved CIP Version 5.

Phase 1: Assessment

The Phase 1 effort starts with an assessment of the existing CIP program (likely Version 3), facilitated by the development and application of a questionnaire intended to create maps of the current systems and processes. The questionnaire includes questions pertaining to the overall health of the system or application in meeting the program needs, the architecture associated with the system, process or application, its regular functioning capabilities, scalability, performance expectations, organization and governance, contract constraints, annual costs to support, skills assessment, support vendor relationship and assessment, constraints affecting any legacy applications, and technology investment plans.

For each system or process, Quanta Technology summarizes the assessment of the existing processes and procedures using a consistent report structure. This evaluation enumerates the strengths and weaknesses of each existing process (CIP Version 3) relative to future (CIP Version 5) needs.

The next step is to perform a needs assessment. This step consists of defining the future state NERC CIP approach and using the results of the current state assessment to determine the activities necessary to achieve the defined future state. This assessment considers the opportunity to enhance existing applications and systems in support of NERC CIP Version 5.

As a first step in the needs assessment, a unified set of CIP Version 5 processes, procedures, policies and performance objectives is specified to be supported based on a contextual
Evolution of NERC CIP  
Continued from page 5

Review and analysis of the framework to support CIP-002-5 and a careful review of each requirement in NERC CIP-003-5 through CIP-009-5, CIP-010-1 and CIP-011-1 standards.

Subject matter experts will then review the usage of these processes, procedures and policies in the current environment and perform a gap assessment relative to the future applicable CIP Version 5 requirements, engaging in a sequential discussion of the topics in the standards.

In the course of this evaluation, we would attempt to answer the following questions:

• What are the current program gaps and risks in migrating to CIP Version 5?
• What are the current state capabilities of CIP staff, processes and technologies?
• What are the desired future state capabilities of the CIP staff, processes and technologies?
• Are there opportunities to automate manual business processes?
• What new tools/technologies/systems should be considered to better support the compliance application or documentation needs?

We begin the review with CIP-003-5 Security Management Controls in order to understand and/or document a set of policies consistent with the desired end-state. Next, due to its importance in the overall design and implementation of the remaining NERC CIP standards, the CIP-010-5 standard, Configuration Change Management and Vulnerability Assessments are reviewed.

Successful implementation of the NERC CIP standards is, in large part, predicated upon establishment of an initial baseline configuration and a well-structured change management process.

Therefore, the review and discussion of these processes at the outset of the project will serve as a baseline as possible controls, systems and tools are considered.

At the conclusion of this needs assessment, the appropriate strategy is determined for each standard and requirement (i.e., outright adoption; retain and transfer favorable aspects into the new process, procedure or policy, or develop an entirely new approach).

A roadmap and high-level project plan to follow to implement the new Version 5 processes and procedures is defined.

Phase 2: Development

The roadmap developed in Phase 1 will define a detailed schedule for developing the processes, procedures and policies necessary to support the NERC CIP Version 5 compliance program. For each area of development, we will implement the strategy identified in the roadmap and project plan and provide for each:

• A policy statement setting the high level intent and expectations
• A process description that describes the workflow and steps to follow, including identification of process owner
• A procedure that denotes specific methods and criteria to be used in meeting the expectations (describes "how")

These will take the form of a preferred document format and will reflect total usage of existing processes, procedures and policies, modified version merging attributes, or completely new documents. For each document developed, we will work with the appropriate resources to:

• Identify ownership of the policies and procedures
• Formalize ownership and review, sign-off and approval processes
• Formalize/review existing document change management processes
• Draft the changed and new documents
• Test the change management, review and approval processes

Finally, we will sequence the development of the processes, procedures and policies in the same order as outlined in the roadmap in Phase 1.
NERC Addresses Physical Security with CIP-014-1 Standard
By Evan Estes, Quanta Technology

A sniper’s April 16, 2013 assault on PG&E’s Metcalf station came as a shock to many in the utility industry and highlighted the vulnerability of the transmission grid. The attack resulted in system operators taking action to avert a blackout and left the station inoperable for 27 days. In response to this attack, on March 7, 2014, FERC issued an order directing NERC to develop reliability standards to address physical security. The result was NERC’s CIP-014-1 standard, which requires Transmission Owners (TOs) to identify critical facilities and then develop, validate and implement plans to protect these facilities.

The CIP-014-1 standard focuses on stations, substations and primary control centers that, if rendered inoperable or damaged due to a physical attack, could result in widespread instability, uncontrolled separation or cascading. Transmission Owners (and potentially, Transmission Operators) are required to go through a six-step process to address compliance with the physical security standard.

1. **Perform a Risk Assessment**
   TOs are required to identify stations/substations (and primary control centers) that meet criteria provided in standard and perform a transmission analysis to determine if or which stations/substations, if rendered inoperable or damaged could result in widespread instability, uncontrolled separation or cascading.

2. **Third Party Verification of Risk Assessment**
   TOs are required to have a third party perform a verification of the Risk Assessment, including:
   a. Certifying the applicability of stations/substations identified in risk assessment
   b. Review of the model used for transmission analysis
   c. Review risk assessment methodology

3. **Notice to Operators of Control Centers**
   TOs will provide notice to Transmission Operators with primary control centers identified in Risk Assessment and verified by third party, that Transmission Operator also has requirements under standard.

4. **Evaluation of Threats and Vulnerabilities**
   TOs and Transmission Operators are required to conduct an assessment of potential threats and vulnerabilities stations, substations and primary control centers identified in Risk Assessment.

5. **Develop Security Plan**
   TOs and Transmission Operators are required to development and implementation a security plan(s) to protect against identified threats and vulnerabilities to the facilities in Risk Assessment.

   TOs and Transmission Operators are required to have a third party perform a verification of the evaluation and the security plan(s) developed.

Timing of compliance with the standard requires TOs to complete Risk Assessments no later than September 30, 2015. Third-party verification of the Risk Assessment is to occur within 90 calendar days of completion of the Risk Assessment or by December 29, 2015. Quanta Technology has developed solutions to support its clients with individual CIP-014-1 requirements, as well as complete compliance solutions for other NERC standards. Questions or inquiries should be directed to Bryan Rushing at (919) 334-3021 or brushing@quanta-technology.com.

---

Join us in Ontario for the grand opening of Quanta Technology’s Sustainable Technology Integration Laboratory (QT-STIL™).

The lab is heavily involved in the testing and engineering analysis of emerging technologies and their integration into distribution systems.

Talk with our Renewables experts and featured speaker, Dr. Damir Novosel, Quanta Technology President and IEEE PES President-Elect.

Quanta Technology QT-STIL™ Laboratory
Open House • Tuesday, October 20

Contact Diana Prkacin at (919) 737-5519 or dprkacin@quanta-technology.com for more information.
Planning & Operational Requirements for Geomagnetic Disturbance
By Ali Daneshpooy and Lisa Williams, Quanta Technology

Geomagnetic Disturbances (GMDs), produced by solar activity and Coronal Mass Ejections (CMEs), result in a shift of the earth’s magnetic field producing DC electric current in power systems, known as Geomagnetically Induced Currents (GICs). These current takes the path of least resistance and, depending on the resistivity of the earth at that given time, location, and network connectivity, several events can occur in electrical power systems:

• Reactive loads
• Voltage collapse
• Tripping/loss of shunt devices
• Power transformer heating
• Saturation of power transformer cores
• Harmonics
• Power system blackout

The following figure demonstrates the general principles contributing to GMD phenomena. The movement of the trapped charged particles in the earth’s magnetic field generates a low frequency magnetic field, which induces quasi-DC current flow, GIC, in a conductive path on earth receptive to those changes.

SOLAR STORMS
GMDs are monitored by the National Oceanic and Atmospheric Administration (NOAA) Space Weather Prediction Center (SWPC) in the United States and by Space Weather Canada in Canada. In the era of the modern power grid, the most significant event occurred on March 13, 1989, resulting in a blackout of the power system in Quebec, Canada due to the tripping of shunt reactive devices. The event began with a solar storm on March 10, 1989. This solar storm created a solar wind that reached the earth in approximately 54 hours.

A GMD can last for several days and has the potential for significant impact on the electric grid and could result in the loss of large portions of the power system from reactive loads and voltage collapse, loss of shunt devices, protection system misoperation due to harmonics, and power transformer heating and damage due to saturation.

Figure 1. Overall mechanism that occurs during GMD
认识到了这并不是一个关于GMD事件是否会发生的问，而是关于何时会发生这样的事件。FERC在2013年发布了一项关于规划和运营要求的提案（FERC Order 779），要求NERC开发可靠性标准，以确保在严重GMD事件期间电力网络的可持续性。最终规则（EOP-010-1）于2014年6月发布，要求传输运营商开发、维护并实施一个操作程序/流程来缓解GMD事件的影响。

NERC对于包括高压侧Y地绕组和终端电压大于200 kV的区域，采用了两阶段的过程：

<table>
<thead>
<tr>
<th>Stage 1 (EOP-010)</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reliability Coordinator</td>
<td>- Develop, coordinate, maintain and implement a GMD operating plan - Disseminating forecast and current space weather information</td>
</tr>
<tr>
<td>Transmission Operator</td>
<td>- Develop, maintain and implement an operating procedure/process to mitigate the effects of GMD events, to include: - Steps/tasks to receive space weather information - System Operator actions to be initiated based on predetermined conditions - Conditions for terminating operating procedures/processes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Stage 2 (TPL-007)</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmission Planners &amp; Operators, Generator Operators, Planning Coordinators</td>
<td>- Assessments/studies of the system for its ability to withstand a Benchmark GMD Event without causing a wide-area blackout, voltage collapse or damage to transformers: - System studies - Transformer impact (reactive power/thermal) - Impact of harmonics on reactive power compensation devices - Mitigation (short-term and long-term solutions)</td>
</tr>
<tr>
<td>Planning Coordinators, Transmission Planners</td>
<td>- Vulnerability assessment (see Figure 2) - Voltage collapse - GIC</td>
</tr>
<tr>
<td>Asset Owners</td>
<td>- Transformer thermal impact assessment, GIC ≥ 75A - Ensure that high-side, wye grounded transformers connected at 200kV or higher will not overheat</td>
</tr>
</tbody>
</table>

*NERC Benchmark GMD Event: http://www.nerc.com/pa/Stand/Project201303GeomagneticDisturbanceMitigation/Benchmark_GMD_Event_Aug27_clean.pdf*

**GMD MANAGEMENT PROGRAM**

一个完整的GMD管理计划应该包括三个关键组件：1）信息和数据收集与系统建模和分析，2）GMD监控程序，和3）GMD缓解计划。

**System Modeling**

Quanta Technology拥有模型电力系统以适应各种磁暴级别并预测将GICs流入电网，并且更重要的是，它们将流入地下的能力。根据特定的模型信息来自客户端（例如，变压器设计，变压器绕组电阻，接地电阻等），我们的GMD专家将使用PowerWorld或PSS/E来模拟GICs。根据建模的场水平和方向，可以确定最易发生的地点，以便于GICs的电力系统进行研究。

*Continued on page 10*
Planning & Operational Requirements for GMD

Continued from page 8

Figure 3 shows the overall approach for transformer modeling. In addition to understanding where the GICs flow and what equipment is vulnerable, it is equally important to consider outage scenarios, evaluate the possibility of voltage collapse, assess the impacts of harmonics on protection systems and review the impact on shunt devices.

Quanta Technology, using additional tools, can provide an analysis of all of these factors:

- **Steady State GMD Analysis**
  - Power World
  - PSS/E
  - GE PSLF
- **Transient Analysis**
  - EMTP-RV
  - PSCAD/EMTDC
- **Network Optimization Tools** (Advanced Studies)
  - Proprietary software

**GMD & GIC Monitoring**

Monitoring the information provided by NOAA through the NERC processes is important to trigger awareness of the possibility of impacts when solar storms are identified that may impact the earth. With a complete understanding of where the GICs will flow and what elements of the power system are the most vulnerable, a GIC monitoring network can be designed and installed to provide engineers and operators specific information about the level of GICs impacting the system during a GMD.

**GMD Mitigation & Operation**

Several defensive options have been considered since the events of March 13, 1989, but hardening the system is the first line of defense against the effects of GICs. Protecting the bulk-power system from a severe GMD requires a multi-layered approach involving planning, design, installation of hardware and systems, training, warning communication, implementation of defensive systems and system restoration.

Possibly the lowest cost and most flexible defensive option to prevent significant damage to the bulk power system from GMDs is to identify critical transmission system equipment that is susceptible to damage and take operative actions in advance of or during the storm, including reducing loading on equipment, reconfiguring the system, and possibly isolating extremely vulnerable equipment.

Quanta Technology can assist with design of operating procedures that can be established to limit the effects of GMD and prevent the flow of GICs at levels that would cause damage.

**CASE ANALYSES: Vulnerability System Assessments**

- **#1 - Assess voltage profile during GMD storm**
  - Field Intensity of 4 V/km
  - Default substation and transformer inputs
  - Transformers not defined in base case, considered to be autotransformers.
  - Storm direction randomly chosen- 90° E

- **#2 - Study of local GIC impact**
  - Multiple storm directions were considered in increments of 10° at a conservative 3 V/km
  - 90° identified as most critical for this particular case; transformer saturation, increased MVar consumption
  - Increased MVar loss results in local issues
  - Impacts of harmonics on equipment control and protection schemes can be estimated using general guidelines, or accurately determined using detailed study.
Quanta Technology was selected for the USTDA funded project, "Technical Assistance for the Smart Grid Upgrades for System Operator and Market Agents in the Dominican Republic". During the course of this project, the Quanta team will conduct an independent evaluation and study to assess the technological, economic, regulatory support and financial aspects of the integration of new smart grid and other technology upgrades needed in the Dominican Republic.

Quanta will consider new technologies that would improve reliability, lower frequency regulation service costs, allow for real-time monitoring and control and enable greater adoption of renewable energy. In August, the team traveled to Santo Domingo for the project kickoff.

For XM in Colombia, Quanta Technology provided technical advice for the conceptual design of two System Integrity Protection Schemes (SIPS) as a continuation of the "Colombian Defense Plans" project. The Quanta team traveled to Medellin, Colombia in May for a workshop and then again in August to present the final results of the project. This project was a continuation of work that Quanta began for XM in 2011 related to developing and implementing additional defense strategies that will protect the Colombian power system against low probability but high impact events. This project defined proposals for the implementation of SIPS which would be then presented to other entities of the Colombian electric power sector.

The Quanta team also developed an implementation plan of the SIPS proposals and recommendations developed during the project with the goal of increasing the national interconnected system (SIN) reliability. XM and Quanta are currently discussing follow up work regarding this important topic.

In May, a team from Joulz visited Quanta Technology’s headquarters in Raleigh, North Carolina, to finalize the "Energized Roadmap" project with Quanta Technology and Quanta Energized Services staff. Quanta provided Joulz with an evaluation of live-line technology options and priorities for Joulz based on market needs, and created a roadmap for Joulz to gain capabilities for energized work activities. The project concluded satisfactorily and the results may become a milestone for the initiation of energized work activities in the Netherlands. Quanta and Joulz staff are currently evaluating the next steps regarding the implementation of this project.
QUANTA TECHNOLOGY’S e-NEWS

WELCOME NEW TEAM MEMBERS

Manuel Atanacio joined the Advisory Services group as an Executive Advisor.

Vahraz Zamani Farahani joined Distribution as a Senior Engineer.

Diana Prkacin joined the Business Development group as Manager, BD.

Twonetta Holden joined us as the Junior Staff Accountant.

Kazi Huq is our Senior Engineer in Distribution & Asset Operations

Chandana Bommareddy joins us as an Advisor in Transmission & Regulatory.

John Johnson is our new Manager, Regulatory in Transmission & Regulatory.

Amin Zamini joined as an Advisor in Distribution & Asset Operations.

David Hart joins us as the new Senior Director of Protection & Control

Zhuoning (Daniel) Liu joins as Senior Engineer, Distribution & Asset Operations

ABOUT QUANTA TECHNOLOGY

Quanta Technology is an expertise-based, independent consulting company providing business and technical expertise to the energy and utility industries for deploying holistic and practical solutions that result in improved performance. Quanta Technology has grown to a client base of over 100 companies with an exceptional staff, many of whom are foremost industry experts for serving client needs.

We are a subsidiary of Quanta Services, Inc., headquartered in Houston, TX, (NYSE: PWR), member of the S&P 500, with 2014 revenues of $7.85 billion. The company is the largest specialty engineering constructor in North America, serving energy companies and communication utilities, according to McGraw Hill’s ECN. More information is available at www.quantaservices.com.

www.quanta-technology.com

UPCOMING CONFERENCES

Oct 5-7  IEEE PES ISGT Latin America (Montevideo, Uruguay)
Oct 11-13 CIGRÉ Grid of the Future (Chicago, IL)
Oct 14-15 NASPI Fall Meeting (Chicago, IL)
Oct 20-21 CEATI Int'l T&D Asset Mgt Conference (Los Angeles, CA)
Oct 20-22 Western Protective Relay Conference (Spokane, WA)

Want to receive our newsletter?

Quanta Technology’s e-News online newsletter is published four times per year, in both electronic and printed form. If you would like to receive your copy, please contact Lisa Williams at (919) 334-3071 or lwilliams@quanta-technology.com.

SHOOTING STAR AWARD

Congratulations to Li Yu!

For significant contributions during Q2 in the area of Distribution.

Vahraz Zamani Farahani joined Distribution as a Senior Engineer.

Manuel Atanacio joined the Advisory Services group as an Executive Advisor.

Twonetta Holden joined us as the Junior Staff Accountant.

Kazi Huq is our Senior Engineer in Distribution & Asset Operations

Chandana Bommareddy joins us as an Advisor in Transmission & Regulatory.

John Johnson is our new Manager, Regulatory in Transmission & Regulatory.

Amin Zamini joined as an Advisor in Distribution & Asset Operations.

David Hart joins us as the new Senior Director of Protection & Control

Zhuoning (Daniel) Liu joins as Senior Engineer, Distribution & Asset Operations

Want to receive our newsletter?

Quanta Technology’s e-News online newsletter is published four times per year, in both electronic and printed form. If you would like to receive your copy, please contact Lisa Williams at (919) 334-3071 or lwilliams@quanta-technology.com.

SHOOTING STAR AWARD

Congratulations to Li Yu!

For significant contributions during Q2 in the area of Distribution.

Vahraz Zamani Farahani joined Distribution as a Senior Engineer.

Manuel Atanacio joined the Advisory Services group as an Executive Advisor.

Twonetta Holden joined us as the Junior Staff Accountant.

Kazi Huq is our Senior Engineer in Distribution & Asset Operations

Chandana Bommareddy joins us as an Advisor in Transmission & Regulatory.

John Johnson is our new Manager, Regulatory in Transmission & Regulatory.

Amin Zamini joined as an Advisor in Distribution & Asset Operations.

David Hart joins us as the new Senior Director of Protection & Control

Zhuoning (Daniel) Liu joins as Senior Engineer, Distribution & Asset Operations

Want to receive our newsletter?

Quanta Technology’s e-News online newsletter is published four times per year, in both electronic and printed form. If you would like to receive your copy, please contact Lisa Williams at (919) 334-3071 or lwilliams@quanta-technology.com.

SHOOTING STAR AWARD

Congratulations to Li Yu!

For significant contributions during Q2 in the area of Distribution.

Vahraz Zamani Farahani joined Distribution as a Senior Engineer.

Manuel Atanacio joined the Advisory Services group as an Executive Advisor.

Twonetta Holden joined us as the Junior Staff Accountant.

Kazi Huq is our Senior Engineer in Distribution & Asset Operations

Chandana Bommareddy joins us as an Advisor in Transmission & Regulatory.

John Johnson is our new Manager, Regulatory in Transmission & Regulatory.

Amin Zamini joined as an Advisor in Distribution & Asset Operations.

David Hart joins us as the new Senior Director of Protection & Control

Zhuoning (Daniel) Liu joins as Senior Engineer, Distribution & Asset Operations

Want to receive our newsletter?

Quanta Technology’s e-News online newsletter is published four times per year, in both electronic and printed form. If you would like to receive your copy, please contact Lisa Williams at (919) 334-3071 or lwilliams@quanta-technology.com.

SHOOTING STAR AWARD

Congratulations to Li Yu!

For significant contributions during Q2 in the area of Distribution.

Vahraz Zamani Farahani joined Distribution as a Senior Engineer.

Manuel Atanacio joined the Advisory Services group as an Executive Advisor.

Twonetta Holden joined us as the Junior Staff Accountant.

Kazi Huq is our Senior Engineer in Distribution & Asset Operations

Chandana Bommareddy joins us as an Advisor in Transmission & Regulatory.

John Johnson is our new Manager, Regulatory in Transmission & Regulatory.

Amin Zamini joined as an Advisor in Distribution & Asset Operations.

David Hart joins us as the new Senior Director of Protection & Control

Zhuoning (Daniel) Liu joins as Senior Engineer, Distribution & Asset Operations

Want to receive our newsletter?

Quanta Technology’s e-News online newsletter is published four times per year, in both electronic and printed form. If you would like to receive your copy, please contact Lisa Williams at (919) 334-3071 or lwilliams@quanta-technology.com.