Proceedings of the 2016 11th International Pipeline Conference
IPC2016
September 26-30, 2016, Calgary, Alberta, Canada

IPC2016-64556

PIPELINE PROJECT TECHNICAL DOCUMENTS CONTROL AND COMPLIANCE

Carolina Pecanha
PAIS LLC
President
Las Vegas, NV, USA

Terry Jansen
Valero VTDC
Director SCADA Integration
San Antonio, TX, USA

Jon Lind
PAIS LLC
SCADA Senior Consultant
Las Vegas, NV, USA

Tatiana Fontes
PAIS LLC
Compliance Consultant
Las Vegas, NV, USA

ABSTRACT

This paper presents an overview of Pipeline Project Technical Documents, along with Control Room Management and Compliance Issues, Challenges and Processes in the Oil & Gas Industry. It will be based on the work that the authors have developed between 2010 and 2015.

With an overwhelming number of standards, norms, and best practices, operational and security requirements needs to be well implemented and documented. Any compliance issues have the potential to cause serious repercussions to an organization as an incident or an audit failure could result in significant financial loss.

This review is especially critical to the industry as it highlights the advantages of taking a broad approach to obtain and maintain compliance in today's Oil & Gas regulatory environment. The focus will be on pipeline monitoring regulations - Department of Transportation (DOT) – Pipeline and Hazardous Materials Safety Administration (PHMSA) and American Petroleum Institute (API) recommended practices: API 1164 (Supervisory Control and Data Acquisition System - SCADA Security), API 1165 (SCADA Displays), API 1167 (SCADA Alarm Management) and API 1168 (Control Room Management).

Regarding Supervisory Control and Data Acquisition Systems (SCADA) security, this includes not only IT infrastructure such as computers and network related appliances, but also other equipment such as programmable logic controllers (PLCs) and Remote Terminal Units (RTUs) depending on the system architecture. The cyber-security threat has become a real issue related to critical infrastructure protection, and physical or human-risk issues. Understanding the systems vulnerabilities that could impact the availability of the control system and the facilities it controls is key.

On the Control Room Management side, current PHMSA regulatory framework, a human factors plan is required to ensure control systems match human capabilities and limitations. Pipeline operators are since required to inform controllers of their roles and responsibilities, and carefully assess the implications on each of the following SCADA areas: alarm management, documentation and procedures, HMI displays, shift handover, fatigue management, change management and training.

Therefore with the pipeline industry facing increasing regulatory scrutiny and ever-increasing cyber-threats, it's more important than ever for companies to improve their plans, documentation, and processes. Companies around the globe are converging and prioritizing Security and Control, establishing long-term strategy to meet and sustain regulatory compliance to remain competitive, increase efficiency and productivity.

The authors, working jointly with the client and industry leaders, have developed compliance methods and procedures to deal with these challenges. After applying these methods and procedures, the observed results were translated into smoother transitions to a centralized SCADA control center, which not only meet regulatory safety guidelines and PHMSA regulation, but also added value and efficiency to the control center operations.

INTRODUCTION

Petrochemical Automation and Integration Specialists consultants have been working with the mid-stream players worldwide. The observations in this space are consistent with wider industry indicators, such as:

- According to a Schlumberger Business Consulting Report from 2012, only 10% of large oil and gas projects ran more than 50% over budget in 1997; by 2011 this figure had nearly tripled to 28% and this trend was expected to worsen. There are many reasons that can contribute for poor project cost control, but certainly one of them is related to the lack of adherence to best practices and documentation.
- The U.S. Department of Transport (DOT) and Pipeline and Hazardous Materials Safety Administration (PHMSA) raised the stakes and increased regulatory exposure. Since 2002, PHMSA has handled more than 600 enforcement actions resulting in nearly $65,000,000 in civil penalties – with an additional $20,000,000 assessed after Department of Justice actions related to the enforcements.

The case for improving both project performance and regulatory compliance is clear. That is the subject of this report and how technical experts have been working with a subsidiary of a leading international manufacturer and marketer of transportation fuels, petrochemical products and power – Valero Terminaling and Distribution (VTDC), a Valero Energy Company, to significantly improve project performance and control room procedures.

At the outset, the client was:

1) Assembling a diverse set of pipelines, terminals, and other logistical assets from different geographies into a new business unit.

2) Consolidating three distinct control rooms each with different procedures and SCADA systems, and

3) Preparing for growth – both organically and via acquisition.

Then part of the corporate IT department, the client SCADA Integration Team, found the typical IT-driven processes and documents to be inadequate in the specialized world of pipeline control/SCADA systems. There was an urgent need to provide a clear, concise, consistent way to communicate control system requirements, specifications, test results, and operating procedures to all involved project participants. With the right processes and documents, everyone from Engineering and Operations to vendors and contractors could get and stay on "the same page". As a result, VTDC now have project processes and documents that help ensure: effective SCADA project execution that all regulatory requirements were met, and result in successful new asset acquisition and handover of the project.

The balance of this document describes the on-going continuous improvement process with summarized into two primary components:

- Project Processes and Documentation – aimed at capturing all the essential information per project including the Cause and Effect, Control Narrative, Operating Manuals and Test Documents.
- Control Room Procedures and Documentation – focused on Alarm management, documentation and procedures, HMI displays, shift handover, fatigue management, change management and training.

As outlined in the following pages VTDC has decreased risk and removed obstacles for safe and efficient operation – providing a firm foundation for the desired corporate growth rate.

NOMENCLATURE

API - American Petroleum Institute
CPM – Computational Pipeline Monitoring
CRM - Control Room Management
DOT - Department of Transportation
ESD - Emergency Shutdown
HAZOP - Hazard and Operability Study
HMI - Graphical User Interface
ICS-CERT – Industrial Control System Cyber Emergency Response Team
I&E - Instrumentation and Electrical
ISA - International Society of Automation
MOC – Management of Change
NIST – National Institute of Standards and Technology
P&ID - Piping and Instrumentation Diagram
PHMSA - Pipeline and Hazardous Materials Safety Administration
PLC - Programmable Logic Controller
RTU - Remote Terminal Unit
SCADA - Supervisory Control and Data Acquisition

PROJECT PROCESSES AND DOCUMENTATION

As stated earlier, the first priority for the client was moving to improve SCADA project processes and documentation. From the SCADA Director's perspective, the basic engineering drawing set was already in place, but was further enhanced to include better, more complete P&IDs – including instrument engineering unit ranges, alarm set-points, and ancillary/cabinet signals (often omitted from 'standard' drawing sets). The P&ID is critical to demonstrate the physical sequence of equipment and systems, as well as how these systems connect. During the design stage, the diagram also provides the basis for the development of system control schemes, allowing for further safety and operational investigations, such as a Hazard and operability study (HAZOP). Additionally, the client defined specific form and content of drawings for PLC wiring, panel layouts, etc.

The P&ID is a key input for the next focus: the Cause & Effect (C&E) matrix – this document is key to SCADA system functionality, providing a concise view of every instrument (such as: pressure transmitters, temperature transmitters, flow

elements, level sensors, analyzers, switches, etc.) along with each associated alarm/event (Causes); and all manual or automated actions (such as: ESD, valve closures, pump stops, interlocks, etc.) (Effects). Working together, the team developed a version of the C&E that is unique in the industry, in that it is:

- Inclusive of *all* instruments and signals, and documents:
  - Instrument engineering unit ranges,
  - P&ID references,
  - Alarm set-points, and delays or special processing requirements
- Sequenced, carefully, in direction of process flow
- Structured to support point-to-point testing
  - Along with retention of test results
- Formatted to be esthetically pleasing

Supplementing the C&E, the next step was to define a standard structure and content for a project Controls Narrative (CN). The CN document expands on the C&E with a succinct discussion of:

- Facility equipment (pipe, pumps, valves, tanks, etc.), including:
  - Equipment descriptions, capacities, operating limits, and hydraulic aspects.
- Automation/Control systems components, including:
  - SCADA Network
  - Each PLC Cabinet, with:
  - A layout of included components.
  - A discussion of any special PLC processing requirements.
- Each Flow Computer, with:
  - A list of attached instruments, and
  - Any special processing requirements.
- An enumeration of all instrumentation and associated parameters
- An enumeration of all Alarms and alarm set-points.

With the desired system requirements and functionality defined by the C&E and CN, it was critical to verify that the system performs as designed. This is accomplished with a comprehensive set of point-to-point test procedures. The use of point-to-point test procedures is designed to verify that equipment is installed and operating as designed, at several levels by checking whether:

- ***Field instruments –*** are operating as specified, wired to the correct terminal locations, and properly calibrated.
- ***PLCs (or RTUs) –*** are correctly acquiring data from the specified field instruments. Processing it correctly to include: engineering units conversion, alarm processing (LOLO, LO, HI, HIHI, or state-change, other types or alarms).
- ***Field HMI Servers & Clients –*** are correctly acquiring data from the PLCs/RTUs. Performing any necessary calculations or comparisons, and displaying the screens, alarm messages, and executing all specified functions as designed.
- ***SCADA Master Station or Host Systems –*** are correctly acquiring data from the PLCs/RTUs. Performing any necessary calculations or comparisons, and displaying the screens, alarm messages, and executing all specified functions as designed.

These tests are normally executed in three stages, with increasing span of coverage:

- **Stage 1:** Spanning PLCs & RTUs through local networks and wiring to Field Instruments.
- **Stage 2:** Spanning Field HMI Servers & Clients through local networks to PLCs/RTUs to Field Instruments.
- **Stage 3:** Spanning SCADA Master Station through wide-area networks to PLCs/RTUs to Field Instruments.

At each stage, completed test documents are retained to support any future investigation or regulatory audit needs.

Finally, to support Control Center operation and Controller training, a standard structure and content for Operating Manuals was defined. These documents are structured around areas or pipeline systems operated, sometimes as a group, by the client's centralized Control Center – and are designed to leverage as much content from the C&E and CN as possible. The typical Operating Manual covers topics, such as:

- General System Description
  - Facility location and access
  - General division of responsibilities
- Site facility description (similar to/leveraged from CN)
- Normal operating procedures
  - Start-up, shut-down, pipeline transfer step-by-step
  - Leak detection considerations
- SCADA operation
  - Display details and examples
- Abnormal operating procedures
  - Alarms, events, indicators – along with operation actions
- Emergency response procedures
- Ancillary information
  - Phone call contact lists
  - Sample reports

All these documents should be considered living documents that will be updated as required throughout the full project life cycle. U.S. regulation mandates that Operating

Manuals be reviewed and updated annually (not to exceed 15 calendar months).

According to VTDC management, the use of this documentation set, and the processes required to develop and approve the content, have been of immeasurable value to completing projects.

CONTROL ROOM PROCEDURES AND DOCUMENTATION

In December 2009, PHMSA published its final regulations on control room management (CRM) in the United States. According to this regulatory framework, a human factors plan is required to ensure control systems match human capabilities and limitations, which also includes fatigue management. Pipeline operators are since required to inform controllers of their roles and responsibilities, and give them adequate process and procedures training. In order to meet the respective requirements of the regulation, operators need to carefully assess the implications on each of the following SCADA areas: alarm management, documentation and procedures, HMI displays, shift handover, fatigue management, change management and training.

As a result of these regulations, and the expedited implementation schedule, there has been a keen interest and intense focus across the industry in ensuring a proper response to the order. Working with the same industry client discussed previously, the team has developed a series of policies and procedures, embodied in a set of documents, to address the technical aspects of the regulations. The 'policy' documents discuss in some detail the company's plans and actions to ensure compliance, while the 'procedure' documents define the specific plans to implement the 'policies'. The table below summarizes the work to-date, and discussion of each document in contained in the ensuing paragraphs:

TABLE 1 - PROCEDURES AND POLICIES BASED ON KEY INDUSTRY RESOURCES

Doc. Type	Subject	Key Industry Resource
Policy + Procedure	Alarm Philosophy	API 1167
Policy	SCADA Cyber-Security	API 1164 TSA Guidelines Corporate Policy
Policy	CPM/Leak Detection	API 1130
Procedure	SCADA Operations & Maintenance	API 1165

Note that, at least in the U.S., the regulations routinely incorporate the American Petroleum Institute (API) standards or recommended practices – either by direct reference or by tacit inclusion in audits and inspection reports. We have found these documents to be key resources for implementing each of the elements.

The first, and most comprehensive of the documents developed jointly with the client was the Alarm Philosophy document. It is intended to be a comprehensive definition of how the company properly handles ways to define, design, implement, maintain, monitor and test alarm systems. The philosophy establishes the company's criteria, definitions, and principles for effective alarm management, including the required procedures or work processes, and metrics used to identify classify, rationalize, prioritize, document, and manage alarms.

This document helps ensure:

- Consistency of alarm design and presentation;
- Consistency of alarms with risk management goals and objectives;
- Agreement with good engineering practices; and
- Effective controller response to alarms.

The philosophy document is designed to meet the federal regulation requirements of 49 CFR 192 and 195 for having a written alarm management plan to provide for effective controller response to alarms.

Next, the continuing emergence of cyber-threats, and emphasis on protecting the country's critical infrastructure – like petroleum pipelines and terminals – focused VTDC's attention on securing the SCADA environment. The Cyber-security document was developed to help in securing the pipeline assets from inadvertent or malicious actions. This SCADA security program provides a means to improve the security of the pipeline SCADA operation by:

- Analyzing vulnerabilities of the SCADA system that can be exploited by unauthorized entities;
- Listing the processes used to identify and analyze the SCADA system vulnerabilities to unauthorized attacks, and;
- Documenting the company practices based on experience and industry best practices, to harden the core architecture.

It is widely expected that U.S. regulators will soon move forward to strengthen required cyber-security practices across the industry – likely incorporating API standard 1164 as model. The plan developed is thorough, complete, and directly aligned with API 1164. It may not be possible to completely prevent all cyber security incidents from occurring, but we believe the current implementation will dramatically reduce risk and mitigate impact.

The last, but not least, of the 'policy' documents addresses pipeline leak detection and Computational Pipeline Monitoring (CPM). Again, the U.S. federal code includes leak detection

provisions and considerations in several sections. Further, regulation requires each computational pipeline monitoring (CPM) leak detection system installed on a hazardous liquid pipeline to comply with API 1130 in operating, maintaining, testing, record keeping, and dispatcher training of the system. To provide a clear reference, the term CPM was developed to specifically cover leak detection using *software-based algorithmic tools*. Simple monitoring tools such as observations of meter over-short reports, observations of pressure deviations and observation of flow rate deviations, without use of an inference engine and alert algorithm, although providing valuable information to the Controller, are not considered to be CPM systems because they do not meet the definition of CPM. The leak detection system used is based around this definition and establishes the framework for the company's alignment with the API 1130 guidance.

The final document in the CRM genre is the SCADA Operations and Maintenance (O&M) manual. It is the "how to" manual that puts the previously described 'policies' into effect. The O&M document contains a lengthy and detailed description of the SCADA implementation – and provides numerous step-by-step procedure – organized as follows:

- SCADA System Overview
- System Architecture
  - Server/network architecture
  - Component details
  - Applications and data propagation
- Standard Operating Procedures
  - Start-up, Shutdown, Re-starts
  - Back-up
  - Etc.
- Business Continuity
  - Offsite cut-over
  - Regular off-site testing
- Management of Change
  - System change approval
  - Code promotion activities
  - Detailed system testing procedures
    - Point-to-point
    - System-to-system
    - Specialized testing for ancillary systems
- Operating system and application version management
  - Patching procedures
- SCADA Cyber-Security
  - Console/system-administrator access
  - Firewall security
  - Vulnerability scanning procedures
  - Anti-virus/malware protection procedures
- Appendices with example procedures and sequences

Certainly having the appropriate content in a similar set of documents goes a long way in preparing the organization to continue safe and efficient facility operations that complies with the regulator's expectations.

As with the project documents, all these documents should be considered living documents that will be updated as required as the systems evolve and new requirements emerge. Further, U.S. regulation mandates that each of these be reviewed and updated annually (not to exceed 15 calendar months).

CONCLUSION

While the structure and content of this paper has focused on the documentation set delivered with the client, the real added value came during the collaboration and discussion needed to develop the documents and procedures. The expectation is to continue this collaborative process assisting in the following:

- *Do the right things*
- *Do them correctly*
- *Document the actions taken*
- *Retain those documents for review and audit*

This combined effort improved project performance considerably. By sharing, discussing and building the set of documents jointly, it also created ownership from the client's perspective and it made the implementation and ongoing work successful and sustainable.

The diagram below shows the results and benefits achieved. Clearly a reliable technical documentation sets the stage for a smoother project transition or pipeline acquisition besides the benefits for a compliance audit. This set of components becomes vital for internal processes and enterprise wide efficiency.

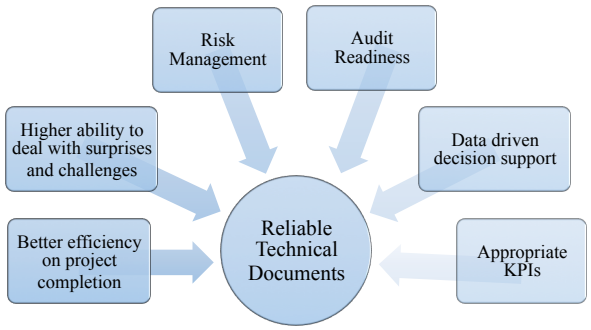

DIAGRAM 1 – RESULTS AND BENEFITS

It is important that all stages from designing to execution to startup and commissioning are properly connected through thorough documentation. If a change occurs in regulation, or a new rule comes along, this customized framework of documents is able to control the change at once. It connects to the company's Management of Change (MOC) procedures.

REFERENCES

API – AMERICAN PETROLEUM INSTITUTE. Computational Pipeline Monitoring. Recommended Practice 1130. Ed. 3. September 2007, R2012.

API – AMERICAN PETROLEUM INSTITUTE. Pipeline SCADA Security. Recommended Practice 1164. Ed. 2. June 2009.

API – AMERICAN PETROLEUM INSTITUTE. Pipeline SCADA Display. Recommended Practice 1165. Ed. 1. January 2007.

API – AMERICAN PETROLEUM INSTITUTE. Pipeline SCADA Alarm Management. Recommended Practice 1167. Ed. 1. December 2010.

API – AMERICAN PETROLEUM INSTITUTE. Pipeline Control Room Management. Recommended Practice 1168. Ed. 2. February 2015.

BYRD, W.R. "New control room management regulations require structured management approach". Pipeline & Gas Journal, v. 237 n. 2, 2010.

ISA – INTERNATIONAL SOCIETY OF AUTOMATION. Alarm system monitoring, assessment and auditing. ISA-TR18.05, 2010.

NTSB – NATIONAL TRANSPORTATION SAFETY BOARD. Supervisory Control and Data Acquisition (SCADA) in liquid pipelines. Safety Study NTSB/SS -05/02. Washington, DC, 2005.

SLONINSKY, J. "Mitigating Risk for Oil & Gas Companies with Project Cost Controls". Oil & Gas Financial Journal, October 2012.

PHMSA – PIPELINE AND HAZARDOUS MATERIALS SAFETY ADMINISTRATION. The Hazardous Materials Regulations, 49 C.