Development and Implementation of Practical Processes for NERC CIP-010 Compliance Evaluation

Tim Chang, Guanhua Wen, Saman Alaeddini, and Daixi Li, *Quanta Technology, LLC.*
Chris Bolton and Lori Marshall, *San Diego Gas & Electric® Company*
Shirin Tabatabai and Tuan Nguyen, *Pacific Gas & Electric*

Abstract—**This paper presents the considerations, challenges, and solutions in the development and implementation of practical processes to enable compliance with CIP-010-4 for Protection and Control departments. The aspects to meeting these requirements, such as strategies for baseline establishment, approaches to obtaining device configuration data, and configuration comparison methodologies, are explored using the real-world experiences of two organizations both faced with significant numbers of BES Cyber Assets that were applicable to the standard. In parallel with the technical and logistical considerations, the actual processes and solutions implemented at these organizations are presented, along with potential future improvements and applications. The real-world experiences of the two utilities discussed in this paper highlight both the aspects that must be considered for the effective development of processes, as well as possible paths for the implementation of solutions to meet CIP-010 requirements.**

I. Introduction

The increasing adoption of digitally-connected communications and hardware technologies in the power systems industry has provided the opportunity for innovative new capabilities to help improve the efficiency, flexibility, and reliability of the power grid. However, the critical role of these cyber assets as well as their inherently accessible nature have raised significant concerns regarding their security and configuration [1]-[2]. Recent intrusion events by non-authorized entities have placed further emphasis on the importance of security considerations for these devices [3]-[4]. NERC CIP-010-4 is a Critical Infrastructure Protection standard that aims to prevent and detect unexpected changes in BES Cyber System configurations through management processes and vulnerability assessments [5].

The standard is comprised of four main requirements:

- Requirement R1 involves the development of management processes to enable identification of deviations in configuration for applicable devices from an expected baseline.
- Requirement R2 calls for the implementation of monitoring processes to enable detection of deviations in configuration for applicable devices from the expected baseline.
- Requirement R3 covers vulnerability assessment processes to ensure proper implementation of cyber security controls and improve security of BES Cyber Systems.
- Requirement R4 involves the implementation of plans for Transient Cyber Assets and Removable Media to address specific aspects outlined in this standard.

The requirements outlined in the CIP-010-4 standard cover a broad range of aspects and applicable devices that fall within the responsibilities of multiple business and operational areas within an organization. Although most of these requirements are typically applicable to Information Technology and Operational Technology departments, certain portions of Requirements R1 and R2 can fall within the responsibility of Protection and Control departments, necessitating an evaluation process to comply with the standard.

This paper explores the considerations, challenges, and solutions associated in the development and implementation of this evaluation process to meet the CIP-010-4 requirements. This exploration draws upon the experiences of the Protection and Control departments of two large electric utilities. These two departments share comparable scope of responsibilities with respect to the CIP-010 standard and opted for similar overall approaches to evaluation methodology, despite a number of differences in technical strategy. The technical and logistical aspects are discussed, as well as possible paths for the implementation of solutions to meet the standard's requirements. Although addressing CIP-010-4 may pose challenges to utilities, resolving the technical and logistical requirements of the standard can open doors to more effectively utilize the potential benefits of the grid's increasingly interconnected digital infrastructure.

II. CIP-010 Requirements and Applicability to Protection and Control

Of the four main requirements outlined in the standard, Requirements R1 and R2 are the portions that are applicable to the typical responsibilities of Protection and Control departments. Requirement R1 is intended to provide the processes to enable identification of deviations in configuration and includes [5]:

- Development of a baseline configuration that covers parameters such as: operating systems and firmware, installed software, logical network accessible ports, and applied security patches (Requirement R1.1).
- Implementation of processes to detect and authorize changes that deviate from the baseline configuration (Requirement R1.2).

- For changes that deviate from the baseline configuration, update the baseline as necessary within 30 calendar days (Requirement R1.3).
- For changes that deviate from the baseline configuration, determine required cyber security controls that could be impacted prior to change and verify that controls are not adversely impacted following the change (Requirement R1.4).
- Where feasible, for High Impact BES Cyber Systems, test changes to ensure that cyber security controls would not be adversely impacted prior to implementing the change (Requirement R1.5).
- If operating system, firmware, or security patches would cause a deviation from the baseline configuration, verify the identify and integrity of the software and source prior to implementing the change (Requirement R1.6).

Requirement R2 is intended to enable detection of deviations from the baseline configuration developed in Requirement 1.1 through periodic (at least once every 35 days) monitoring processes. This requirement is applicable to High Impact BES Cyber Systems, defined under CIP-002 as Control Centers or backup Control Centers used to perform specified functional obligations [6].

Of the conditions stated above, R1.1, R1.2, and potentially R1.3 were determined to be within the scope of responsibility for the Protection and Control departments discussed in this paper. Determination of the requirements of CIP-010-4 is dependent on the scope of devices to be considered as well as the content of the baseline configurations. Requirement R1 states that BES Cyber Systems and their associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets that are classified as “High Impact” or “Medium Impact” [6] under CIP-002 are applicable. Further, according to R1.1 the baseline configurations for these applicable devices must contain the operating systems and firmware, installed software, network accessible ports, and security patches of applicable devices.

The definitions for Medium Impact BES Cyber Systems include transmission facilities 500kV and above, or 200kV and above that are connected to multiple lines, as well as some generation and interconnection facilities, Special Protection Systems, and Remedial Action Schemes. Of interest to Protection and Control is the scope of applicable devices, which specifically includes protection systems for system equipment, breaker failure, and current, frequency, speed, and phase-based devices [6].

Combining the above, the scope of Requirement R1 can be stated as any protection device connected to BES levels (typically 200kV and above) that has a software-based configuration or network port. The timing considerations of Requirement R1.3 and R2 may also apply, requiring baseline configurations to be updated within 30 days of change implementation and device configurations to be checked against the baseline every 35 days for High Impact BES Cyber Systems.

Other requirements, such as the verification of cyber security controls (R1.4), testing of High Impact BES Cyber System configuration changes prior to implementation (R1.5), vulnerability assessments (R3), and plans for Transient Cyber Assets and Removable Media (R4) typically fall outside the responsibility of the Protection and Control departments and are addressed by other operating units within the organization.

III. Addressing CIP-010 Requirements

The scope identified in the previous section requires the capability to identify deviations from a baseline configuration for the applicable devices, and to update baselines within a set time to accommodate changes. To implement this scope, the following technical and process considerations must be addressed:

- Establishment of a baseline configuration for applicable devices.
- Comparison of device configurations against the baseline configuration. This will require the sources of data for both baseline and device configurations to be identified and a methodology to perform the actual comparison to be defined.
- Tracking to ensure addressing of deviations from baseline within 30 calendar days.
- Provisions for repeatability of above process on a periodic basis (every 35 days) for High Impact BES Cyber Systems.

A. Establishing a Baseline

The establishment of a baseline configuration requires consideration for three main aspects:

- Identification of contents of a baseline configuration.
- Strategy for the organization of baselines.
- Format and recordkeeping of the baseline configurations.

The required contents of a baseline configuration are specified in Requirement R1.1, which include the operating systems and firmware, installed software (custom or otherwise), network accessible ports, and security patches of applicable devices. Due to the limited nature of the software implemented in most protection, control, and communication devices applicable to the standard, the two most common relevant configuration points are the firmware and network accessible ports.

The scope of devices applicable to Protection and Control may cover a significant number of different device models, each with their own configuration settings and data formats. Even devices of the same model may be utilized for different applications that necessitate different configurations. A strategy for the organization and classification of baselines is needed to enable effective comparison against the range of devices and applications.

The most straightforward strategy for baseline organization segments the configurations by device type, forcing all devices of a certain model to abide by a single configuration for firmware and network ports, as shown in Fig. 1. This strategy promotes standardization and is relatively simple to implement, reducing the effort required for tracking changes to configuration (Requirement R1.3) and for managing the baselines. However, configuration flexibility may be lost when considering different applications and use cases, resulting in a greater count of deviations and increase in effort required for the review, authorization, and documentation of these deviations. (Requirement R1.2).

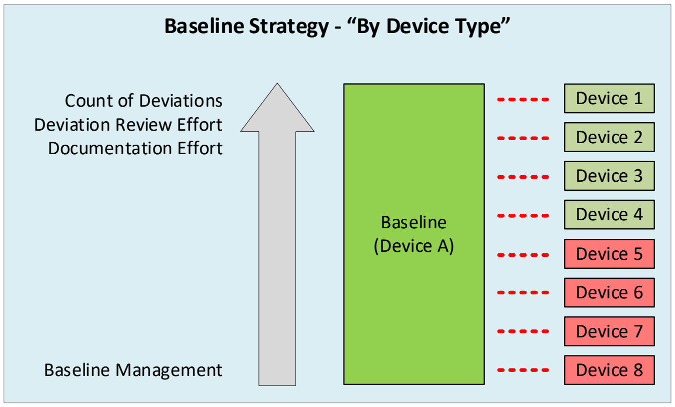


Fig. 1. Baseline configurations organized by device type

As an alternative to the simple but rigid device type approach to baseline organization, a modified strategy could organize and classify baselines according to both device type and application, as shown in Fig. 2. This approach provides for greater configuration flexibility in meeting use cases, which result in fewer cases of deviations and subsequent effort for review, authorization, and documentation.

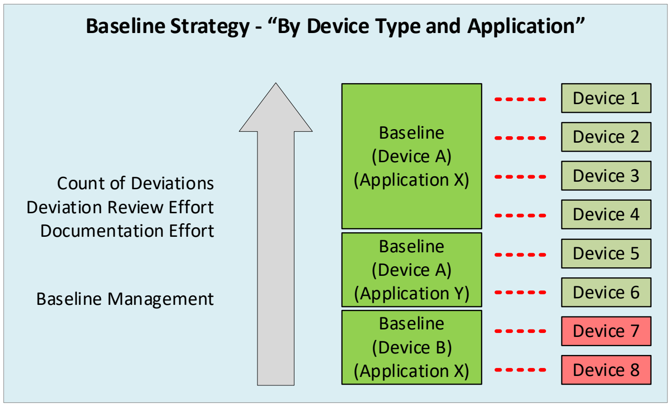


Fig. 2. Baseline configurations organized by device type and application

In contrast to the organizational strategies presented above, the definition of a separate baseline configuration for each device instance, as shown in Fig. 3 promotes effectively infinite flexibility for device type and application. Under this approach, each individual device can be compared against a unique baseline configuration best suited for its particular use case. This can reduce the number of deviations, and the associated effort required for review, authorization, and documentation of these deviations (Requirement R1.2).

However, since each device has a potentially unique baseline, this strategy requires greater effort for the management of configurations. In addition, this approach can also introduce fragmentation of configurations, even among similar use cases.

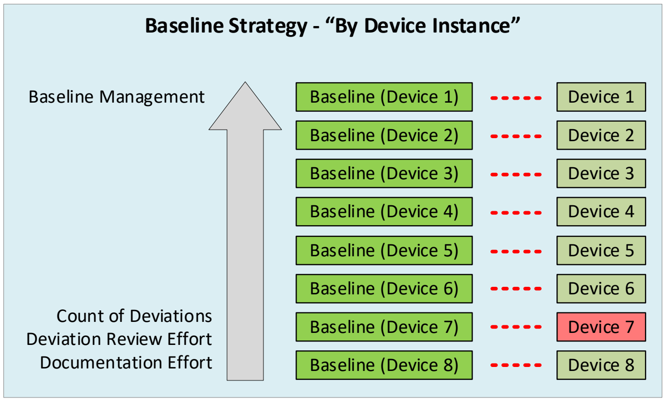


Fig. 3. Baseline configurations organized by device instance

No single approach will fit the needs and practices of all utilities. The strategy selected by any particular organization would need to offer enough granularity to cover their devices and applications, while also addressing the required number of devices, protection philosophies, logistical capabilities, and engineering resources.

Finally, the format and form of recordkeeping of the configurations must be considered in establishment of the baseline. This refers to both how the configurations are recorded as well as how they are stored and managed, which can range from straightforward spreadsheets to dedicated database applications. Although the CIP-010-4 standard does not directly impose any requirements on the form and format of the baseline, the use of these for periodic comparison of configurations may benefit from consideration for the accessibility, interactability, and management of the records.

B. Sources of Data for Detecting Deviations in Configuration

To detect deviations from the established baseline configurations, the configuration of applicable devices would need to be compared against the baseline records. This requirement forms the primary actionable component of the CIP-010-4 scope applicable to the typical Protection and Control department. The practical processes to enable comparison of all applicable devices on a periodic basis may impose a number of challenges to engineers, including issues with obtaining data or the potentially significant number of applicable devices that need evaluation. The two main aspects of consideration are:

- The sources from which the data for device and baseline configurations will be obtained.
- The methodology for comparing the configurations to determine any deviations from the baseline.

The source of data used to obtain baseline configurations is directly related to the consideration for form and formats stated in the previous section, which can range from spreadsheets to database records within custom applications. The source of data used to obtain configurations for applicable devices will depend on an organization's data and communications infrastructure, recordkeeping practices, and approach to comparison. Ideally, configuration data would be obtained directly from the devices deployed in the field. However, this approach may not presently be practical for most organizations due to the number of devices applicable to the standard and lack of ubiquitous communications infrastructure to retrieve settings from each device. Without the capability for routine remote extraction of device settings on a large scale, crew may be required to physically retrieve configuration data if on-device settings are required.

As an alternate approach to obtaining configuration data from the devices themselves, the utilization of representative records may be more feasible for most organizations. These records may include electronic settings files or documentation of the device configuration such as settings sheets. However, use of data that was not directly taken from the devices in the field may carry the potential risk of the records not properly representing the actual configuration of devices. In particular, configuration records may be out of date or missing entirely if gaps exist in settings management practices. These concerns can largely be mitigated through effective processes in handling device settings and leveraging existing infrastructure such as the relay settings repository to both maintain records in one central location and impose controls on the management processes.

C. Comparison Methodology for Detecting Deviations in Configuration

Once the data sources from which the comparison is to be performed have been identified, a methodology to perform the actual comparison is required. Although straightforward in concept, the form and format of the configuration data will have a major influence on the comparison methodologies which may be adopted.

The simplest approach would be a manual comparison of the relevant device settings against the configurations specified in the baseline. This methodology effectively has no constraints on the form and format of the data, aside from accessibility in viewing the settings and configurations. Since this approach relies on the judgement of the reviewing engineers, the efficiency is dependent on the experience and capabilities of personnel as well as the ease of viewing the data. Due to the number of devices that require review, this approach can impose significant burden on engineering resources and may not be a practical approach for most organizations.

Software-assisted comparison methodologies, through scripting or application approaches, are compelling alternatives to purely manual reviews. These approaches are well suited to the repetitive nature of the required CIP-010 evaluation tasks, both in terms of comparing large numbers of devices, and in enabling the comparisons to be easily repeatable.

However, software-based approaches impose a number of prerequires to operate effectively and reliably, particularly in the form and format of the data. First, both the baseline configuration records as well as the device settings need to be available in software-readable formats, which may be a concern for relay settings files of some device types. Next, the data must be accessible, which may require extraction processes depending on the baseline and device settings storage infrastructure. Third, the comparison mechanisms need to be compatible with both the data sources as well as the data formats, meaning that the software would need to be able to interpret the settings fields within the baseline and device configurations to make the comparison. This may require additional built-in logic within the comparison mechanism, as more feature-rich microprocessor-based devices may feature dependencies between settings (ports or elements may be dependent to an "Enable" field, for example).

Finally, in addition to the requirements to enable software-assisted comparisons of individual settings and baselines, consideration must also be given to the batch evaluation of large number of devices. Even more so than the comparison of individual devices, the evaluation of multiple devices would benefit greatly from software integration that enables smooth extraction of data and comparison of configurations. Existing software tools provided by device vendors are typically designed to focus on one device instance at a time and may not be suitable for batch review of multiple settings across different device types, applications, and manufacturers. Further, they typically require the user to provide the data for comparison, necessitating that engineers first extract the data from the storage infrastructure. Custom-developed software can resolve these issues but require design and development expertise that may not be inherently available to some organizations.

D. Tracking Changes

For changes that deviate from the baseline configuration, Requirement R1.3 states that baselines must be updated within 30 days to reflect the change. This requirement imposes a tracking mechanism to implemented for the CIP-010 evaluation process. If a database or software-based storage infrastructure is used to record the baseline configurations, this tracking requirement can be built as a function to notify engineers of impending 30-day deadlines.

IV. Implementing Solutions

Faced with the technical and logistical considerations discussed in Section III, the Protection and Control departments of two large utilities implemented solutions based on their unique protection practices, existing infrastructure, and forward-looking philosophies. Both organizations opted for software-based approaches for the evaluation of the CIP-010 requirements within their scope.

Although software-based solutions imposed a number of additional requirements such as data accessibility, data format readability, and additional logic in the comparison methodology, they could also reduce the effort required by engineering personnel and offered easy repeatability of the evaluation process. Both utilities were well positioned to accommodate the needs of software-based approaches due to their previous efforts and experience in the use of scripting and tools to assist in the evaluation of compliance requirements.

A. Baseline Establishment

The implementation of the baseline configurations, including content, organizational strategy, and format of records and storage, was performed based on the settings philosophies and existing tool infrastructure of the two utilities. For one organization, the philosophy for port configurations was based on defined settings templates for each device type and application. Since the port settings would be expected to adhere to a specified standard, this organization could limit their comparison scope for CIP-010 to only those ports that were expected to change from device to device. This existing segmentation of settings templates was directly applied to the organization of baseline configurations, reflecting the “by device and application” strategy discussed in Section III and representing the minimum number of different baselines that cover the required device types and applications. A custom database application was developed by this utility to store and manage the baseline configurations, and to facilitate the accessibility and data needs of the software-based approach for comparison of configurations.

For the other organization, the philosophy for port configuration was based on providing engineers with maximum flexibility to adapt to requirements of each device instance. By default, all communications ports are disabled in the relay settings templates, requiring engineers to set them according to the specific use case. Since engineers have greater control over the settings, each port setting is tracked in the comparison scope for CIP-010. This approach to the relay settings is carried through to the baseline organization strategy, reflecting the “by device instance” method discussed in Section III. Since each device instance is effectively its own baseline configuration, this utility opted to define baselines as the last deployed relay settings record and utilize the relay settings file as the baseline record. This approach leveraged the existing relay settings repository infrastructure as the form of storage and enabled the use of the built-in tracking and administration controls to facilitate management of the baselines.

B. *Data Sources*

The selection of data sources used for the configuration comparison closely follows the form and format of the baseline records described in the previous section. One organization developed a custom database application to store and manage their baseline configurations, and the other defined their last deployed relay settings file to contain the baseline configuration for each device instance. In both cases, the storage mediums provided support for the management of the data records and extraction of the data to external applications, enabling integration with the configuration comparison mechanism to form a seamless process.

To represent the deployed device configurations, the settings record within the relay settings repository was utilized by both organizations. While obtaining actual deployed settings would have been preferable, the logistical challenges associated with remote data extraction made that approach impractical on the scale required by the scope of applicable devices. Both organizations relied on their existing settings deployment process to ensure that the latest setting with “As-Left” status represented the devices in the field. As in the case of source data for baselines, the use of the settings repository provided support for data extraction to external applications as part of an integrated process for configuration comparison.

C. *Comparison Methodology*

Both utilities adopted software-assisted approaches for the comparison of deployed settings against the baseline record to determine any deviations. While the content to be compared may have differed between organizations the overall processes were similar in the implemented compliance evaluation solutions.

First, baseline configuration data was obtained from the designated source, which could have been either the custom database application or the relay settings repository. Since both sources supported integration with external applications, the required data could be directly extracted by the implemented software solution without requiring manual efforts by the engineers.

Next, the settings files under review were extracted from the relay settings repository. Similar to above, integration of the compliance evaluation software with the repository enabled the required settings files to be obtained automatically.

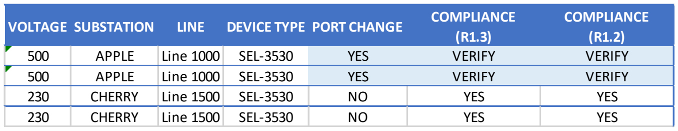
Although the two utilities evaluated different content – one only compared the ports that were expected to change from device to device, while the other included all ports in their comparison due to the flexibility given to their engineers – the comparison routines contained within the evaluation solutions of both organizations were designed to read the various settings files formats and determine whether applicable parameters deviated from the baseline configuration. When necessary, additional logic was implemented to accommodate settings dependencies (such as “enable” fields) unique to each device type.

D. *Output Review and Evidence*

Both utilities implemented the output of the configuration comparison in the form of summary spreadsheets. While their most direct role is enabling engineers to review comparison results to identify deviations, these sheets are also intended to serve documentary evidence for proof of compliance with the CIP-010 standard.

Similar to other compliance evaluation documentation implemented at the two organization, the CIP-010 output follows a hierarchical structure covering high-level summaries down to detail comparison for each applicable configuration field. This multi-level approach to documentation provides engineers with the ability to quickly determine the state of their evaluation scope, as well as to dig deeper into the details to investigate configuration deviations. This is particularly relevant when multiple devices are studied, making system-wide evaluations feasible.

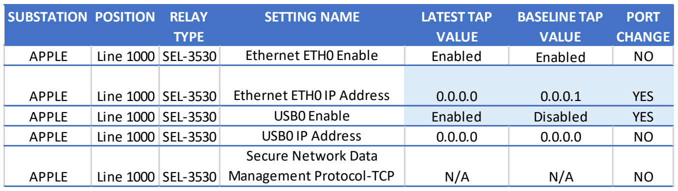
An example of the high-level summary tab of the output for one of the organizations is shown in Fig. 4. Here, the critical evaluation verdict of compliance with R1.2 (compare configurations) and R1.3 (update baselines) is shown for each device in the small study scope. Although this example only included four devices, this summary can easily be expanded to encompass the entire system of devices applicable to CIP-010.



VOLTAGE	SUBSTATION	LINE	DEVICE TYPE	PORT CHANGE	COMPLIANCE (R1.3)	COMPLIANCE (R1.2)
500	APPLE	Line 1000	SEL-3530	YES	VERIFY	VERIFY
500	APPLE	Line 1000	SEL-3530	YES	VERIFY	VERIFY
230	CHERRY	Line 1500	SEL-3530	NO	YES	YES
230	CHERRY	Line 1500	SEL-3530	NO	YES	YES

Fig. 4. Summary Tab of Evaluation Output

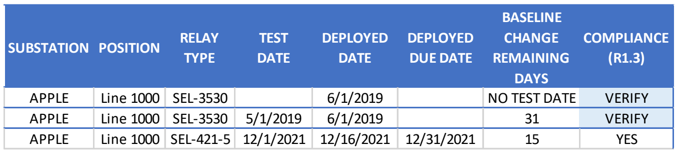
For the cases identified as having deviations in configuration, a tab containing a list of all configuration parameters being evaluated allows engineers to quickly pinpoint which specific fields deviate from the baseline. As shown in Fig. 5, the configuration fields which differ from baseline to latest deployed are highlighted, with the contents provided.



SUBSTATION	POSITION	RELAY TYPE	SETTING NAME	LATEST TAP VALUE	BASELINE TAP VALUE	PORT CHANGE
APPLE	Line 1000	SEL-3530	Ethernet ETH0 Enable	Enabled	Enabled	NO
APPLE	Line 1000	SEL-3530	Ethernet ETH0 IP Address	0.0.0.0	0.0.0.1	YES
APPLE	Line 1000	SEL-3530	USB0 Enable	Enabled	Disabled	YES
APPLE	Line 1000	SEL-3530	USB0 IP Address	0.0.0.0	0.0.0.0	NO
APPLE	Line 1000	SEL-3530	Secure Network Data Management Protocol-TCP	N/A	N/A	NO

Fig. 5. Tab of All Device Comparison Fields

To track that baseline updates occur according to requirements, another tab shows the deployed date against the baseline update date. This enables engineers to track down issues associated with R1.3, as shown in Fig. 6.



SUBSTATION	POSITION	RELAY TYPE	TEST DATE	DEPLOYED DATE	DEPLOYED DUE DATE	BASELINE CHANGE REMAINING DAYS	COMPLIANCE (R1.3)
APPLE	Line 1000	SEL-3530		6/1/2019		NO TEST DATE	VERIFY
APPLE	Line 1000	SEL-3530	5/1/2019	6/1/2019		31	VERIFY
APPLE	Line 1000	SEL-421-5	12/1/2021	12/16/2021	12/31/2021	15	YES

Fig. 6. Tab of Baseline Updates

Although these functions could also be provided through the comparison application's interface, outputting to spreadsheet form at a specific time enables archiving of the documentation for proof-of-compliance purposes. External to these outputs, the use of database applications in the management of the baseline configurations can further assist in identifying, tracking, and notifying engineers of needed baseline updates.

E. *Overall Process*

The software-based solutions implemented at the two utilities offer the capability to efficiently identify deviations from established baseline configurations for the devices applicable to the Protection and Control departments. Both organizations leveraged software-based applications for data storage, translation, configuration comparison, and reporting, enabling the CIP-010 evaluation process to be readily repeated as needed.

The overall process for one of the organizations is shown in Fig. 7. It can be seen that the baseline configurations are stored in a custom database application and device settings within the settings repository. Both databases transfer their data to the evaluation application, which performs the comparison. A report can be generated containing the results of the comparison, which is especially useful when multiple devices are evaluated.

One of three actions may be taken to address any identified deviations:

- The setting in question may be modified to match the baseline configuration.
- The baseline configuration itself may be updated to reflect the changes from the setting.
- The deviation may be authorized and an explanation for the configuration change provided.

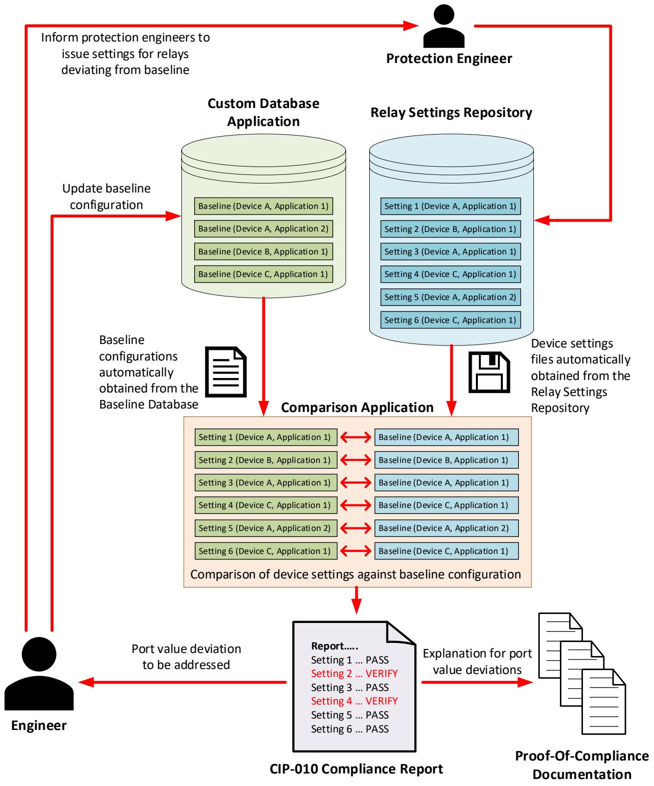

Inform protection engineers to issue settings for relays deviating from baseline
Protection Engineer
Custom Database Application
Relay Settings Repository
Update baseline configuration
Baseline (Device A, Application 1)
Baseline (Device A, Application 2)
Baseline (Device B, Application 1)
Baseline (Device C, Application 1)
Setting 1 (Device A, Application 1)
Setting 2 (Device B, Application 1)
Setting 3 (Device A, Application 1)
Setting 4 (Device C, Application 1)
Setting 5 (Device A, Application 2)
Setting 6 (Device C, Application 1)
Baseline configurations automatically obtained from the Baseline Database
Device settings files automatically obtained from the Relay Settings Repository
Comparison Application
Setting 1 (Device A, Application 1) ⟷ Baseline (Device A, Application 1)
Setting 2 (Device B, Application 1) ⟷ Baseline (Device B, Application 1)
Setting 3 (Device A, Application 1) ⟷ Baseline (Device A, Application 1)
Setting 4 (Device C, Application 1) ⟷ Baseline (Device C, Application 1)
Setting 5 (Device A, Application 2) ⟷ Baseline (Device A, Application 2)
Setting 6 (Device C, Application 1) ⟷ Baseline (Device C, Application 1)
Comparison of device settings against baseline configuration
Port value deviation to be addressed
Report.....
Setting 1 ... PASS
Setting 2 ... VERIFY
Setting 3 ... PASS
Setting 4 ... VERIFY
Setting 5 ... PASS
Setting 6 ... PASS
Explanation for port value deviations
Engineer
CIP-010 Compliance Report
Proof-Of-Compliance Documentation

Fig. 7. Process flow of implemented solution for one organization

The overall process for the second organization is shown in Fig. 8. It can be seen that the baseline configurations are defined as the previous setting file for each device instance and are stored within the settings repository. The evaluation application performs the comparison, automatically obtaining the required settings data from the repository. A report can be generated containing the results of the comparison, which is especially useful when multiple devices are evaluated.

In addition to the direct evaluation of CIP-010 requirements, this utility also incorporated the software-assisted evaluation capability into their relay settings process. Since their baseline configurations are defined as the latest deployed settings of a device instance, any change to settings for any device are checked against the baseline to monitor for any changes to port or firmware parameters.

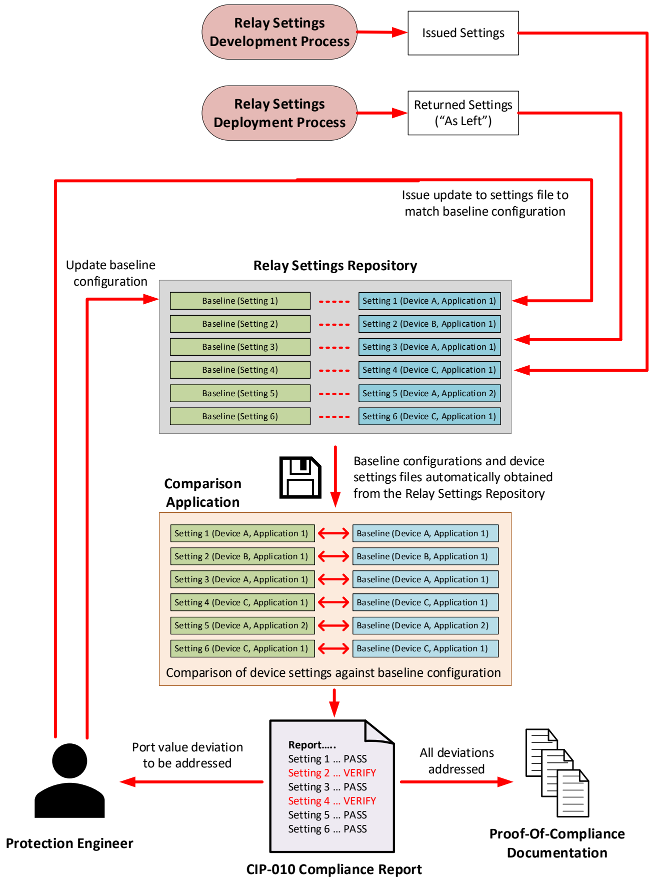

Relay Settings Development Process
Issued Settings
Relay Settings Deployment Process
Returned Settings ("As Left")
Issue update to settings file to match baseline configuration
Update baseline configuration
Relay Settings Repository
Baseline (Setting 1)
Baseline (Setting 2)
Baseline (Setting 3)
Baseline (Setting 4)
Baseline (Setting 5)
Baseline (Setting 6)
Setting 1 (Device A, Application 1)
Setting 2 (Device B, Application 1)
Setting 3 (Device A, Application 1)
Setting 4 (Device C, Application 1)
Setting 5 (Device A, Application 2)
Setting 6 (Device C, Application 1)
Comparison Application
Baseline configurations and device settings files automatically obtained from the Relay Settings Repository
Setting 1 (Device A, Application 1)
Setting 2 (Device B, Application 1)
Setting 3 (Device A, Application 1)
Setting 4 (Device C, Application 1)
Setting 5 (Device A, Application 2)
Setting 6 (Device C, Application 1)
Baseline (Device A, Application 1)
Baseline (Device B, Application 1)
Baseline (Device A, Application 1)
Baseline (Device C, Application 1)
Baseline (Device A, Application 2)
Baseline (Device C, Application 1)
Comparison of device settings against baseline configuration
Port value deviation to be addressed
Report.....
Setting 1 ... PASS
Setting 2 ... VERIFY
Setting 3 ... PASS
Setting 4 ... VERIFY
Setting 5 ... PASS
Setting 6 ... PASS
All deviations addressed
Protection Engineer
CIP-010 Compliance Report
Proof-Of-Compliance Documentation

Fig. 8. Process flow of implemented solution for the other organization

V. Improvements and Future Work

Although the implementations discussed in this paper make feasible the evaluation of an entire system of device configurations, the reliance on the settings within the repository representing the settings in the field is the aspect that is most likely to cause potential issues for the compliance evaluation process. Utilization of these stored settings is currently the best representation of the actual device configurations since downloading field settings at the scale required is typically not feasible. However, the power systems industry – including the utilities represented in this paper – are moving to improve their communications and infrastructure to make the routine downloading of field settings and device monitoring data a reality.

For actual implementation, mass real-time data comparison or analysis with field settings may still be beyond the communications and infrastructure capabilities. However, the available remote access to field settings can better ensure that configuration records actually match those deployed on field devices.

When applied to CIP-010, this removes one of the most significant potential issues in the existing evaluation process. Beyond CIP-010, this capability could also be applied to other cybersecurity standards such as CIP-007, of which Requirement R1 covers the consideration and documentation of ports and services for applicable devices [7]. Similar to the configuration comparisons of CIP-010, comparison of relay protection settings could confirm the proper application of intended settings. Routine remote access capabilities to field devices is a natural extension of the digital transformation processes utilities have been undergoing for years, with applications reaching far beyond CIP-010.

VI. Conclusion

The CIP-010-4 compliance standard covers a broad range of aspects and applicable devices that fall within the responsibilities of multiple business and operational units within an electric power utility. The aspects that apply to the typical Protection and Control department primarily involve the management processes stated in R1, requiring the establishment and management of baseline configurations and the identification of devices that deviate from these baseline configurations. Applicable devices consist of those identified as High Impact or Medium Impact BES Cyber Systems.

In addressing these requirements, technical and logistical aspects must be considered such as: the content of the baselines, organizational strategy, form and format, comparison methodology, and process repeatability. The approach taken to meet these requirements will typically reflect an organization's settings philosophy, existing infrastructure, engineering resources, and experience with software-based solutions.

The practical solutions to the requirements implemented by the two utilities discussed in this paper are built around the considerations noted above, with differences in settings philosophies having a major impact on the baseline strategies and forms. Both organizations adopted software-based approaches to compliance evaluation according to their preferences for the optimization of capabilities of their engineering staff, requirement for processes to be readily repeatable, and previous experience with scripting to assist in evaluation and data transformation tasks.

The resulting solutions offer a framework for the implementation of compliance evaluation processes to enable efficient (and repeatable) identification of deviations from established baseline configurations for devices applicable to the Protection and Control departments. One potential improvement to the solutions discussed in this paper would be to directly obtain device settings from their deployed hardware rather than relay on settings records. Although this is presently impractical for most organizations due to logistical challenges for the necessary scale, improvements to communications and control infrastructure in the future may make mass retrieval of remote configurations viable. Aside from CIP-010 evaluation, reliable and routine real-time access to deployed relays could have major implications on the interaction and utilization of relay devices.

References

[1] S. Ward et al., "Cyber Security Issues for Protective Relays; C1 Working Group Members of Power System Relaying Committee," *2007 IEEE Power Engineering Society General Meeting, 2007*, pp. 1-8, doi: 10.1109/PES.2007.385583.

[2] T. Sukumara, J. Starck, J. Vellore, E. Kumar and G. Harish, "Cyber security — Securing the protection and control relay communication in substation," *2018 71st Annual Conference for Protective Relay Engineers (CPRE)*, 2018, pp. 1-7, doi: 10.1109/CPRE.2018.8349788.

[3] I.G.Macola, *The five worst cyberattacks against the power industry since 2014*, Power-Technology.com, April 2020. [Online]. Available:

https://www.power-technology.com/features/the-five-worst-cyberattacks-against-the-power-industry-since2014/

[4] North American Electric Reliability Corporation, “Lesson Learned Risks Powed by Firewall Firmware Vulnerabilities", Atlanta, GA, USA, 2019. [Online]. Available: https://www.nerc.com/pa/rrm/ea/Lessons%20Learned%20Document%20Library/20190901_Risks_Posed_by_Firewall_Firmware_Vulnerabilities.pdf

[5] *Configuration Change Management and Vulnerability Assessments*, NERC Critical Infrastructure Protection Standard CIP-010-4 and Application Guideline. [Online]. Available: https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-010-4.pdf

[6] *BES Cyber System Categorization*, NERC Critical Infrastructure Protection Standard CIP-002-5.1a and Application Guideline. [Online]. Available: https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-002-5.1a.pdf

[7] *BES Cyber System Categorization*, NERC Critical Infrastructure Protection Standard CIP-007-6 and Application Guideline. [Online]. Available: https://www.nerc.com/pa/Stand/Prjct2014XXCrtclInfraPrtctnVr5Rvns/CIP-007-6_CLEAN_06022014.pdf

BIOGRAPHIES

Tim Chang received his MASc from the University of Toronto and has been with Quanta Technology since 2009. His experience at Quanta Technology has covered broad range of aspects from traditional transmission and distribution engineering applications to use of real-time simulators for advanced renewable impact studies. He has been a major contributor to the development of automated processes and applications for data management and engineering studies, including evaluation of NERC compliance standards, software modeling solutions, and wide-area protection coordination studies.

Guanhua Wen received has BASc from the University of Waterloo and has been with Quanta Technology since 2016. His experience at Quanta Technology has included protection modeling, software design, and project management. He has developed, and has lead development of software to solve problems specifically for the power industry. His focus is to develop and grow a software team to bring modern software solutions to the power industry. Guanhua has worked on large-scale projects with major electric utilities in North America and internationally.

Saman Alaeddini received his MASc from Ryerson University and has been with Quanta Technology since 2009. He leads the engineering automation team at Quanta Technology that has developed many innovative software-based solutions for the power systems industry, particularly in the area of NERC compliance evaluation. Saman is a specialist in protection system modeling, database management and analysis, autonomous systems design, robotics, and industrial processes. He has been involved in wide-area protection projects for over 7000 transmission lines with 10 large electric utilities in North America and internationally.

Daixi Li received her MASc from North Carolina State University and has been with Quanta Technology since 2016. Her main research focuses are volt/VAr control and cost-benefit analysis based on detailed utility circuits. At Quanta Technology, she has worked on wide-area coordination studies, CAPE model validation, automated naming convention updates, and programmed tools to aid engineers managing substation point list reports.

Chris Bolton is manager of system protection automation and control engineering at SDG&E®, where he has worked since 2011. Bolton has held a variety of positions with the utility, including in substation engineering, capital projects, substation technical analysis and support, and system protection maintenance. Bolton graduated with a BSEE degree from California State Polytechnic University, Pomona and is a licensed professional engineer in California.

Lori Marshall is a Senior Transmission Compliance Advisor within System Protection Automation & Control engineering at SDG&E. Lori has worked at SDG&E since 2002 and has held a variety of positions within the utility, including Fleet Services, Transmission and Planning, and Reliability and Analysis. Lori holds an AA in Information Technology from the University of Phoenix and specializes in database administration, automation, workflow processes for distribution and transmission settings, capital project process documentation, and NERC compliance.

Shirin Tabatabai currently works in the System Protection group at Pacific Gas and Electric Company as a Manager of Technical Support. In her current role she is responsible for tracking the protection assets and ensuring compliance with applicable regulatory requirements as well as supporting the interconnections with third party generators. Ms. Tabatabai has over 20 years' experience in the Electric Utility Operations. She plays an active role in recruiting new engineers to PG&E from across the country to help ensure the most robust and talented workforce in place. Ms. Tabatabai helped found PG&E's W-STEM group in 2012 which is an organization dedicated to recruiting, developing and retaining talented in the disciplines of science, technology, engineering and mathematics at PG&E.

Tuan Nguyen currently works in the System Protection group at Pacific Gas and Electric Company as a Compliance Specialist, Principal. This position is the lead for providing much-needed support to keeping us compliant with existing and everchanging NERC CIP standards and enhancing the many tools used for storing records. Tuan began his career at PG&E in 2007 as a Transmission Specialist in the Test Department after completing his Bachelor of Science degree in Electrical Engineering from Sacramento State University. He had been a significant contributor to Substation Test Department technical support part of his career and also implemented RTS/Power Base automated testing tools to streamline consistent testing and documentation systemwide to meet NERC PRC-005 standard.