CIP-010 R1: The Importance of Baseline Configuration as a Critical Security Management Control

Purpose

CIP-010 brings into the CIP Regulations baseline configuration management as a way to reduce or eliminate security gaps resulting from Cyber Assets that are not properly configured. These gaps occur when baseline changes are not documented, when required changes (such as security patches) are not implemented, and when configuration change mandates are not implemented on one or more Cyber Assets. The security gaps are clearly cyber security vulnerabilities that can be exploited. This paper discusses different approaches to this challenge and how best practices can be employed to eliminate security gaps for the Bulk Energy System (BES).

Introduction

The NERC-CIP standards are the primary knowledge resource used by the Utility industry to ensure our nation's power grid is protected from unintentional (accidental) and intentional (malicious) disruption. While the NERC-CIP standards take a comprehensive approach to cyber security, there remain areas where the specific implications of security vulnerabilities are not understood by the industry at large. This whitepaper looks at the specific areas of Cyber Security – Security Management Controls as covered by NERC-CIP-010.

What is Baseline Configuration Management?

Each Cyber Asset stores electronic configuration files and/or records. This configuration information includes:

- Functional settings that determine how the asset operates
- Versions of software currently installed (includes BIOS, firmware, operating system, applications, etc.)
- Patches (including security patches) that are installed
- Ports that are active for normal and emergency operations and how they are configured
- Services that are enabled

While configuration information is not limited to this list, these are the primary information categories covered by CIP-010-05 because they are an important part of determining the security of each asset.

Baseline configuration is a snapshot of the configuration at a specific time. For example, if we retrieved the configuration for a server or router that information is a snapshot of how the device was configured at the time we retrieved it. This is what is meant by baseline configuration. Producing an actual baseline requires that the configuration information come from the asset itself as this is the only definitive source of this information.

Baseline configuration management involves periodically retrieving the configuration of the asset and comparing it to the baseline. If no changes have occurred, no action is required. If one or more changes have occurred, the change(s) must be assessed, verified, and documented or rolled-back to the baseline configuration.

Practical Application of Baseline Configuration Management

The practical application of baseline configuration management involves a process to systematically control assets to a defined configuration state known to be the "most secure" configuration.

This process is defined with CIP-010 regulation, explicitly calling out primary security issues that include operating systems, security patches, software versions, logical ports, system services, and firmware.

The overriding purpose is to maintain cyber asset configurations at a known state that has the highest level of security. While the regulation calls out specific areas that need to be part of the baseline configuration management practice, it should not be construed as a definitive list. Any configuration elements that can impact or impose a security issue should be included in the overall practice.

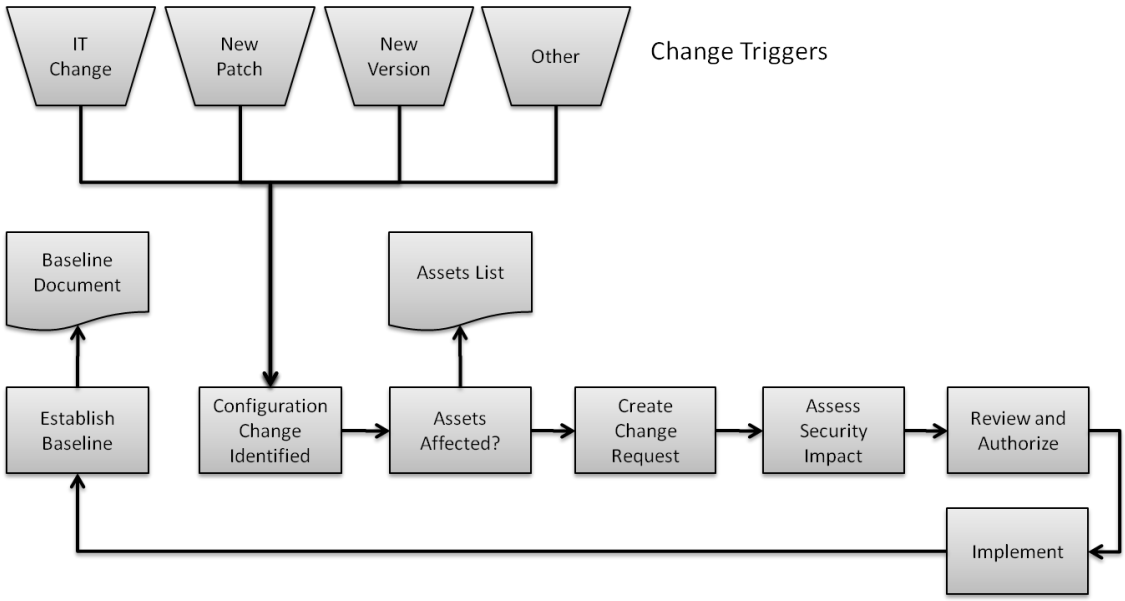
The process behind baseline configuration management has these elements:

1) Establish a known secure baseline for each asset
2) Periodically collect the current configuration and compare it to the baseline
3) If available – verify that the volatile and permanent configurations are the same
4) Identify any changes between the two configurations
5) Create a change request for any changes that are not rolled-back
6) Assess cyber security controls that could potentially be impacted by the change
7) Review and Authorize the change (Change Advisory Board)
8) Update the baseline configuration per authorized changes

Baseline Configuration Management – External Triggers

The following diagram provides an overview of the process for controlling assets to a defined, "most secure" configuration. The process depicted here deals with triggers that will require a change to be made in configuration of one or more IT assets.

Baseline Configuration Management Process (External Triggers)



In this process, potential changes are identified and then reviewed prior to being implemented. An important point is the need to determine the list of assets affected by the change. For example, in the case of a security patch the list of assets is likely to be all assets of a certain brand, model number or product family.

Assessing the security impact is an entire sub-process performed when assessing the security impact of a proposed change to ensure there are no "knock on" security impacts (any application or other asset that depends on the device, operating system, application being patched). This could result in additional configuration changes that must also go through the baseline management process. Conflicting security patches or changes must all be considered in this assessment.

This process assumes that all changes, and their impact to the overall BES, will be assessed and approved before they are implemented. However, one of the most important capabilities of baseline configuration management is identifying when changes occur that have NOT gone through the above process, or that have not been implemented as planned. This requires a different process to be followed.

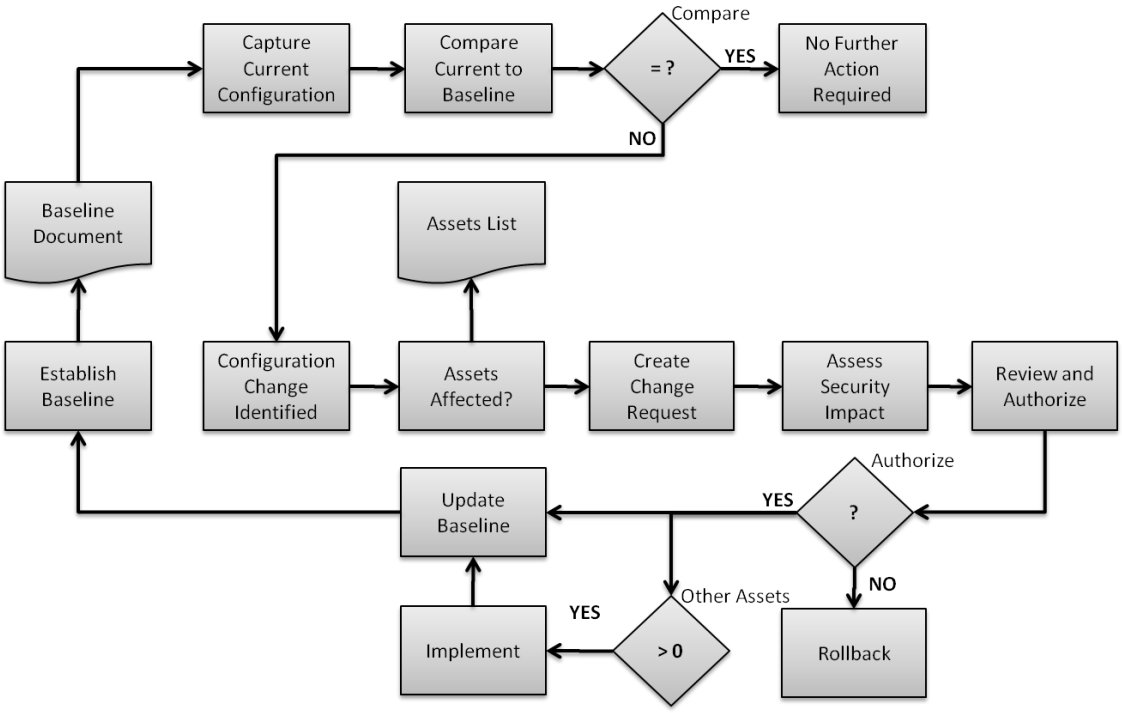
Baseline Configuration Management – Issue Detection

CIP-010-05 requires that cyber security overseers authorize and document any changes to the configuration of cyber assets. Any changes not properly authorized and documented could become an alleged violation of CIP-010-05 to minimize adverse effect to the reliable operation of the Bulk Electric System.

In essence, any unauthorized or undocumented configuration change is considered an unauthorized BES Cyber Security modification. This includes authorized changes that are not implemented and those implemented but that fail to successfully complete. For example, a security patch could be installed on an asset that fails to properly complete its installation. This would leave the asset in a compromised state.

The following diagram provides an overview of the process for detecting and resolving unauthorized changes and for validating authorized changes:

Baseline Configuration Management Process (Issue Detection)



This process requires the comparison of the current configuration of an asset to its approved baseline in order to determine if any unauthorized changes have been made or any authorized changes have not been made (or completed successfully).

When the configuration comparison does not match, the difference(s) must be evaluated by the change review and approval process (just like in the external triggers process). If the changes are valid, we accept the configuration and it becomes the new baseline configuration. If the changes are not valid, we know what has changed so that we can take the actions necessary to configure the asset properly by rolling the device back to the approved baseline configuration.

It is also important to understand who changed the asset outside the approved configuration management process. Identifying the privileged actor that made a change outside of the approved process provides the opportunity for training to ensure the process is followed in the future – or to take corrective actions if such is deemed necessary and appropriate.

Severity of the Cyber Security Threat

The best way to understand the cyber security threat imposed by not managing the baseline configuration of cyber assets is to recognize that any cyber asset that does not have the proper configuration has a security vulnerability that can be exploited. Considering that security patches are a primary trigger for updating a baseline, this becomes even more onerous as information about security patches typically resides in the public domain – making them a prime area for exploit.

Risk

The risk that baseline configuration management addresses is characterized by opportunity and impact. The impact is severe due to the fact that a cyber asset could be compromised, with significant probability that doing so would provide an exploit path into many areas of the BES. This is easy to understand.

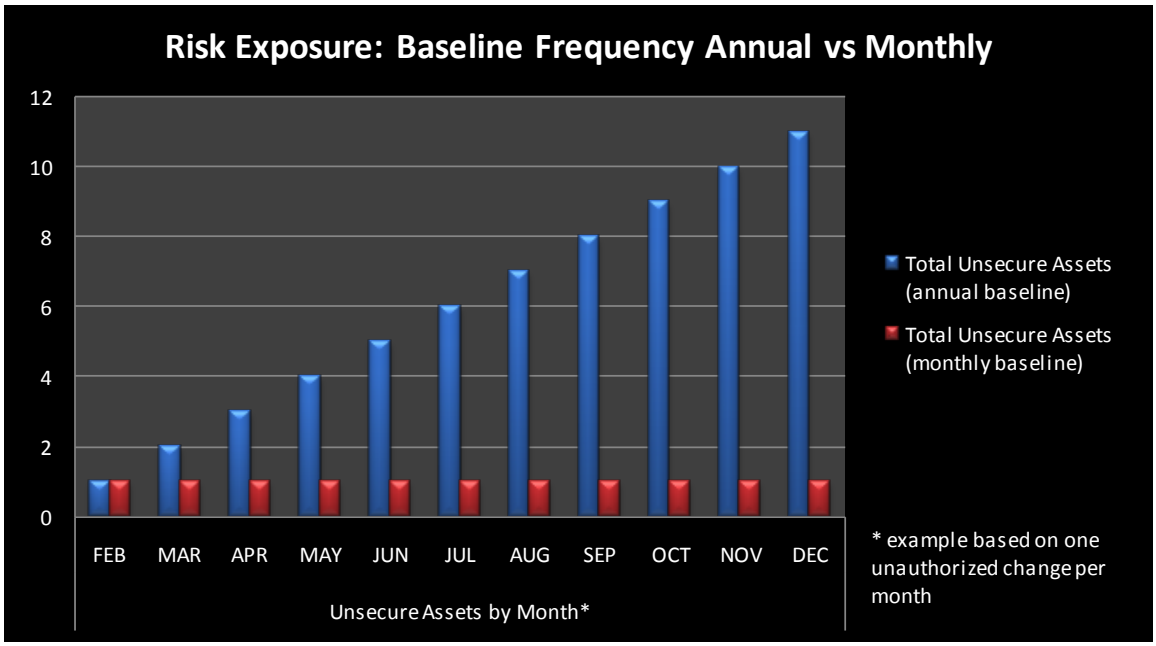
What is often missed in assessing this risk is the opportunity for exploit represented by this issue. That is influenced by two factors:

1) The number of assets (i.e. – all cyber assets)
2) The length of the "risk window"

Obviously the first factor, the number of cyber assets, cannot be controlled. Whatever cyber assets are in place determines this portion of the risk opportunity.

What we can control is the risk window. The risk window is the elapsed time from the point where a cyber asset does not have the proper configuration until such time as it once again does have the proper configuration. In simpler terms, the risk window is the length of time the asset is at risk. This can vary quite dramatically.

For example, let's compare an annual baseline configuration management practice to a monthly practice. In this example we assume (for simplicity) that one (1) unauthorized change occurs each month.



This example demonstrates how risk exposure is affected by the baseline frequency. The gap between baseline cycles is risk occurs. In the gap, risk accumulates to include all unauthorized changes until the next baseline cycle is run. For an annual cycle the length of the risk window is one year. For a monthly cycle, it is one month. For a daily cycle it is 24 hours.

The important point is that the risk to the BES can be controlled, and it is controlled by the frequency in which we perform baseline configuration management.

Best Practice Guidance

The best practice guidance for configuration ports is that they should be treated just like any other security concern in regards to active monitoring and control. The steps that should be taken include:

1) Insure that all configuration ports are connected to an out-of-band or management specific network
2) Segregate the out-of-band network from the normal or production network(s)
3) Institute role-based access and control over all configuration ports (restrict access, least privilege)
4) Encrypt communications to configuration ports (where supported by devices)
5) Use proper or multi-factor authentication to configuration ports
6) Persistently monitor all configuration ports to ensure all access meets the security policy
7) Log all access to configuration ports by each actor
8) Log all privileged user activity over configuration ports
9) Alert and ALARM on specific messages or events detected on the access port.

One reference that can help in assessing or designing a secure out-of-band network is available from the Defense Information System Agency:
http://iase.disa.mil/stigs/downloads/pdf/network_management_security_guidance_at-a-glance_v8r1.pdf

Various hardware and software solutions exist for managing the out-of-band network per the best practice guidance provided above. These solutions should be evaluated against existing security policies and wherever possible be capable of directly supporting them programmatically to limit the scope of manual policy enforcement.

About This Whitepaper

The best practice guidance for baseline configuration management is that the security vulnerabilities should be proactively managed through technology with direct support for the two processes outlined in this paper. Without supporting technology, these processes are manpower intensive and subject to human error.

The best practice for effectively controlling the risk window definitely requires automation. Manually collecting, recording, and assessing all of the configuration data on cyber assets is labor-intensive and may introduce inadvertent errors. In most cases, running a monthly or weekly baseline would be prohibitively expensive. With automation the baseline frequency can easily be supported as a routine security validation function to improve the security posture and be audit ready at any time.

The other best practice recommendations are:

1) Capture, document and secure baseline data programmatically (eliminate human error)
2) Perform comparisons programmatically and determine where differences exist (eliminate human error)
3) Provide a change control portal for implementing configuration changes, logging who, what and how an asset was patched. A complete change session log
4) Generate alerts when mismatches are found and review with the privileged actor that made the change (process improvement)
5) Document the approval process
6) Run comparisons frequently if technically feasible
7) Force rerun immediately after approved changes are made (validation)
8) Produce reports that detail all changes (and their dispositions)
9) Review reports for patterns that can improve the practice

Various hardware and software solutions exist that can help meet these challenges. These solutions should be evaluated against organizational context and specific requirements for the different asset types in place in order to cover the broadest asset footprint possible – keeping in mind exceptions will require manual baseline configuration management.

Full Disclosure

This whitepaper was written and produced by TDi Technologies, a software vendor that provides an out-of-band software solution to the Utility industry and other vertical markets. The information presented here represents our best understanding of the security issues associated with configuration ports, which is a problem area our company focuses on. The whitepaper is intended to provide useful and educational content that can assist Utility companies in providing secure, dependable power to our Nation without interruption.

Future Whitepapers

If you would like to receive additional whitepapers on NERC-CIP from us as they become available, please email us at info@tditechnologies.com