NERC CIP Alignment

Executive Summary

Utilities are currently weighing the advantages of increasing IP connectivity across all levels of operations against the costs of regulatory compliance. Meeting NERC CIP standards is a costly effort in terms of implementation, verification and potential penalties. Moving forward, utilities must implement network architectures that balance the benefits of connectivity modernization with the cost and effort required to meet regulatory compliance. The ideal approach will facilitate compliance and at the same time enhance operational integrity, availability, and resiliency at an acceptable Total Cost of Ownership.

The Tempered Networks solution automates connectivity and network security for distributed devices over trusted and untrusted network infrastructure. Our technology is based on the International Society of Automation (ISA) TR100.15.01 architecture model for the creation and management of private overlay networks. When considering its use within a NERC regulated utility, the Tempered Networks solution is used to create flexible Electronic Security Perimeters (ESPs) for distributed equipment and facilitates the use of Electronic Access Control and Monitoring Systems (EACMS) for connectivity into these distributed ESPs.

The Tempered Networks solution can be deployed in regulated electric utility environments in order to achieve the business objectives often associated with increased connectivity, while also facilitating and reducing the labor cost of compliance with NERC CIP standards. Most importantly, our solution does more than just facilitate compliance; it provides real and demonstrated security hardening, resilience, and awareness. The Tempered Networks solution can be deployed as a transparent drop-in solution with minimal disruption and performance impact to existing operations, and it can be managed by Operations and/or IT groups.

Tempered Networks facilitates NERC CIP compliance by:

1. Creating flexible Electronic Security Perimeters (ESPs) for distributed facilities and equipment
2. Facilitating the use of Electronic Access Control and Monitoring Systems (EACMS) for connectivity to Cyber Assets within these ESPs
3. Centralizing governance, auditing, monitoring, logging, change control, and documentation of these Access Points and their associated configurations
4. Introducing user authentication, authorization, and auditing for remote access to Cyber Assets without increasing complexity, therefore allowing network architectures that provide additional flexibility for other technologies
5. Enabling ad-hoc networks for managing assets through test, patch, upgrade, remediate, and replacement phases

Tempered Networks Theory of Operation

A Tempered Networks environment is comprised of a scalable orchestration engine (HIPswitch Conductor), industrial and data-center grade security appliances (HIPswitches) and a management console and user interface (SimpleConnect).

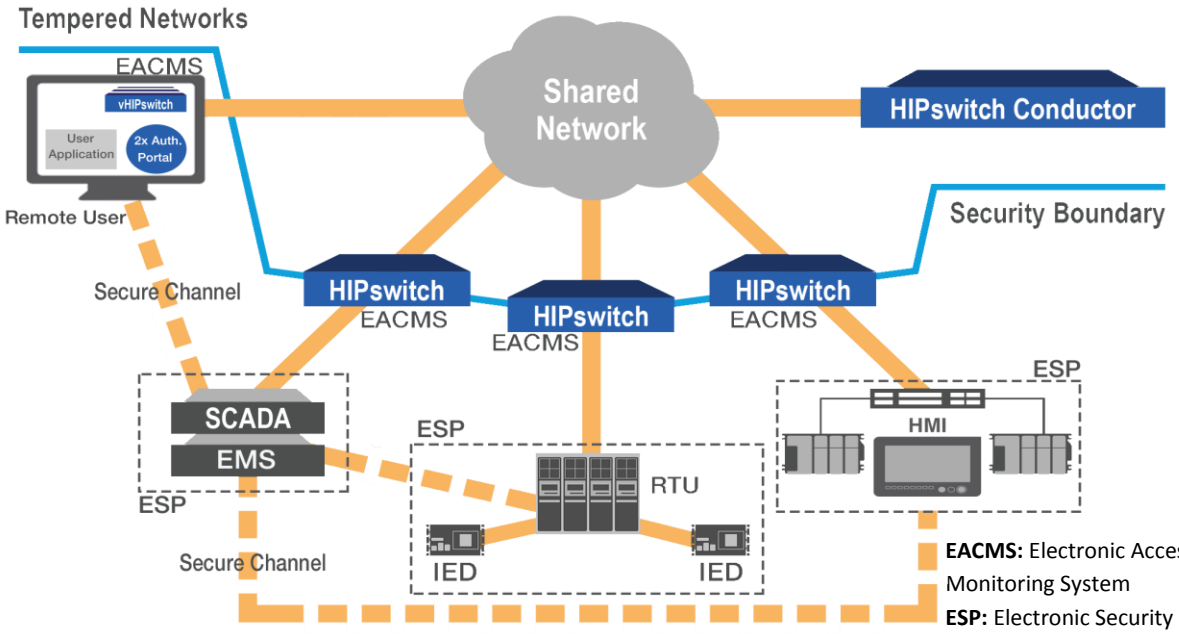

FIGURE 1: EXAMPLE PRIVATE OVERLAY NETWORK

EACMS: Electronic Access Control and Monitoring System
ESP: Electronic Security Perimeter
RTU: Remote Terminal Unit
EMS: Energy Management System
IED: Intelligent Electronic Device

Secure Communications

Tempered Networks HIPswitches connect to a WAN infrastructure using standard network services and interfaces. HIPswitches establish point-to-point and point-to-multipoint encrypted HIP tunnels to implement a private overlay network, and apply additional network policy controls over device communications that traverse each HIPswitch. Several independent private overlay networks can be managed by the HIPswitch Conductor. Each private overlay network can be delegated to different users, yet the governance of the entire solution is centralized and retained by the administrator. The Tempered Networks solution therefore provides the enterprise with an internal, on-demand, "Private Networks as a Service" capability. Users interact with a Tempered Networks solution through SimpleConnect, a management console and graphical user interface.

Each HIPswitch has a unique cryptographic identity in the form of an RSA 2048-bit key pair. A private overlay network is simply a whitelist of HIPswitch cryptographic identities. The list of identities is provided to the members of each private overlay network, and each HIPswitch authenticates and authorizes peer HIPswitches against this whitelist of allowed peers. This architecture provides a trust model that minimizes unauthorized communications. Communications policies are tightly integrated with HIPswitch cryptographic identities, reducing the time and complexity of the full lifecycle (issuance through revocation) management associated with network security and access credentials.

Network Management Interface

The HIPswitch Conductor maintains a secure management channel to each HIPswitch, based on the Trusted Computing Group Interface for Metadata Access Points (IF-MAP). IF-MAP provides a graph-based Configuration Management Database (CMDB) and acts as a clearinghouse for security policy and configuration metadata, and uses a publish/subscribe semantic to deliver real-time metadata updates to subscribed HIPswitches. TCG has specified Metadata for Industrial Control Systems (ICS) Security to standardize the management channel between the HIPswitches and the HIPswitch Conductor. The management channel avoids the need for physical presence of the HIPswitch in order to manage the full lifecycle of HIPswitch configuration.

Each HIPswitch must be initially provisioned with one or more HIPswitch Conductor instances, and once a HIPswitch is managed by the HIPswitch Conductor, an explicit management trust relationship is established. Likewise, the HIPswitch Conductor also maintains a whitelist of managed HIPswitches that are allowed to connect to the HIPswitch Conductor IF-MAP service. In this manner, the HIPswitch Conductor centralizes the configuration, monitoring, and governance of the HIPswitches.
SimpleConnect is a web-based user interface that exposes APIs to integrate the HIPswitch functions with additional business and security applications such as SIEMs, network and physical access control, and identity provisioning.

Private Overlay Network Communications

A HIPswitch acts as a bump-in-the-wire device that connects to a shared WAN infrastructure on one (or optionally several) network interface and a Local Area Network (LAN) segment with a second network interface. Additional interfaces can connect local serial equipment as IP endpoints within the LAN that are remotely accessible through the private overlay network. The HIPswitch can also NAT and route for the local equipment as it transits the overlay network. Furthermore, the HIPswitch can enforce layer 3 Stateful Packet Inspection rules. The addition of confidentiality, integrity protection, and traffic inspection adds latency and jitter, with increases of <1ms to 1.8ms RTT depending on the HIPswitch model.
The configuration of each HIPswitch is managed centrally via the SimpleConnect user interface, and the configuration metadata is associated with the cryptographic identity of the HIPswitch, providing high assurance that a specific HIPswitch (and only that specific HIPswitch) can provide the provisioned network access and policies. Local device communications are monitored and logged. Logs are stored both locally (log size varies depending on HIPswitch model) and can be forwarded to central log services.

Remote Access

A significant challenge with NERC compliance is credential management for access to cyber assets. While the use of a jump host adds an initial layer of user authentication, there is a subsequent gap in authentication services to devices behind ESPs. It can be very difficult to add managed authentication services into these environments, especially for the many devices that do not support user authentication and authorization. HIPswitches can enforce user authentication and provide an authorization framework for managed access to BES cyber assets. Remote access should nevertheless follow the guiding principle of least privilege, which in this case implies that remote access should be

granted to just the minimum required device or devices and for only the duration necessary to perform the remote access tasks. Furthermore, application policies (firewall rules) should be implemented to limit remote access connectivity to just the specific policies required for successful task performance. HIPswitch policies can be defined and refined at a very granular level with very little effort, while logging all configuration changes and access events.

Tempered Networks Key Features for NERC Regulated Utilities

Tempered Networks is deployed as part of a defense in depth security architecture that facilitates NERC CIP Compliance:

1. Communications Security
    a. Default-Deny policies
    b. Communications confidentiality
    c. Communications integrity protection
    d. SPI Firewall inspection
    e. Certificate and key lifecycle management
        i. Issuance and revocation
    f. Secure serial-Ethernet encapsulation
2. Change Management
    a. Configuration of central log service for HIPswitches and HIPswitch Conductors
        i. Failed and successful authentication attempts
        ii. Authenticated user actions
        iii. HIPswitch communications activity
        iv. Device communications activity
    b. Centralized Firmware management of HIPswitches
    c. API-driven management layer
        i. Configuration
        ii. Obtaining status
3. User Authentication and Authorization
    a. Role-based access model
    b. Assignment of user-based remote access policies
    c. Ability to disable admin account on the HIPswitch Conductor
    d. No user access to individual HIPswitches
4. No administrative interfaces on HIPswitches
5. Systems Documentation
    a. Structured and free-form data fields for documentation
        i. ESPs
        ii. Access Points
        iii. CAs and CCAs
        iv. Access Policies
    b. Network whitelisting enforces documentation of connected devices

Tempered Networks Facilitates NERC CIP Compliance

As of the current draft of this document, the current NERC CIP Standards are version 3, while CIP Standards version 5 are currently pending regulatory approval. Since this whitepaper is a living document, ongoing work will be required to monitor FERC regulatory actions for ongoing changes and to update this section accordingly.

In the sections below, version 5 of the CIP Standards is considered with respect to the features available in Tempered Networks solution. Some CIP Standards are not considered applicable and are listed only to be fully inclusive.

Description or Requirement	Tempered Networks Applicability to Requirements
CIP-002-5.1: BES Cyber System Categorization	
CIP-003-5: Security Management Controls	
CIP-004-5.1: Personnel and Training	
CIP-005-5: Electronic Security Perimeter(s)	
R1: Electronic Security Perimeter	
R1.1: BES Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP	BES Cyber Assets on the protected side of a HIPswitch reside within an ESP.
R1.2: All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	A HIPswitch is the EAP for external connectivity to / from an ESP.
R1.3: Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	The Tempered Networks solution operates on the principle of network whitelisting. All communications must be explicitly allowed. All other access is denied by default.
R1.4: Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	The Tempered Networks solution does not support dial-up connectivity, but it does support authentication for remote network access.
R1.5: Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	The Tempered Networks solution logs network connectivity flows for allowed communications. These logs can be integrated with a SIEM for increased monitoring and visibility.
R2: Interactive Remote Access Management	
R2.1: Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	The Tempered Networks solution can be used to restrict connectivity between an Intermediate System (jump host) and the specific Cyber Assets needed for the Interactive remote support session.
R2.2: For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	The Tempered Networks solution provides end-to-end encryption.
R2.3: Require multi-factor authentication for all Interactive Remote Access sessions.	The Tempered Networks solution can be configured to enforce an authentication mechanism for Remote Access.

CIP-006-5: Physical Security of BES Cyber Systems	
CIP-007-5: Systems Security Management	
R1: Ports and Services	The Tempered Networks solution can be used to prevent Cyber Assets from having External Routable Connectivity, which can remove Medium Impact BES Cyber Systems from the requirements in this standard. The components of the Tempered Networks solution do fall under this standard, however Tempered Networks has been designed for deployments within these contexts. Tempered Networks provides documentation of required ports and services and a justification for the port and service.
R1.1: Enable only network ports that have been determined to be needed	The Tempered Networks solution works on the principle of network whitelisting. Once the HIPswitch Firewall has been enabled, all network ports must be explicitly allowed.
R1.2: Protect against use of unnecessary physical I/O ports	Tempered Networks HIPswitches have no exposed USB or video ports. The Serial console port is logically locked unless configured for serial-IP encapsulation.
R2: Security Patch Management	
R2.1: Patch management process for applicable Cyber Assets	The Tempered Networks solution facilitates a patch management process for BES Cyber Assets by enabling connectivity to remote assets. Tempered Networks provides security patches for the Tempered Networks components, along with the necessary information to assess and evaluate the impact of patches and instructions for testing and applying them.
R2.2: Evaluate security patches for applicability	The Tempered Networks product suite involves a minimized, hardened firmware that limits exposure to 3rd party vulnerabilities. As part of the Tempered Security Development Lifecycle (SDL) program, Tempered Networks conducts internal and independent assessments and evaluates vulnerabilities for applicability to our products and promptly communicates relevant findings to our customers.
R2.3: Apply patches, create mitigation plan, or revise mitigation plan	Tempered Networks provides their customers with security patches that are applied via the SimpleConnect user interface, or at individual HIPswitches.
R2.4: Implement mitigation plans	The Tempered Networks solution can be used to manage isolation or connectivity for cyber assets as part of mitigation plans.
R3: Malicious Code Prevention	The Tempered Networks solution does not run a system for Malicious Code detection or prevention

	(Anti-Virus). Tempered Networks can provide a letter of vendor attestation to this effect.
R3.1: Deploy methods to deter, detect, or prevent malicious code	A Tempered Networks deployment can constrain connectivity to deter propagation of malicious code.
R3.2: Mitigate threat of detected malicious code	A Tempered Networks deployment can facilitate the isolation of Cyber Assets.
R3.3: Update detection methods that require signatures or patterns, including testing	
R4: Security Event Monitoring	
R4.1: Log events at BES Cyber System level or at Cyber Asset level	HIPswitches log detected network communications between ESPs as permitted by their security policies. The Tempered Networks solution also logs both successful and failed login attempts.
R4.2: Generate alerts for security events when necessary	The Tempered Networks solution can be integrated with a SIEM to provide alerts based on communications activities of Cyber Assets between ESPs.
R4.3: Retain event logs for at least 90 days	The Tempered Networks components can forward log messages to a central syslog service to comply with this requirement. (Secure syslog available in 2015)
R5: System Access Control	
R5.1: Enforce authentication of interactive user access	HIPswitches can be configured to require user authentication prior to enabling communications policies for access to cyber assets within ESPs.
R5.2: Identify and inventory enabled accounts	The SimpleConnect default admin account can be disabled. SimpleConnect user accounts are centralized and each user has a unique login ID. Integration with Active Directory / LDAP is available. The HIPswitches do not have any admin or individual enabled accounts.
R5.3: Identify individuals who have access to shared accounts	When the Tempered Networks solution is used to constrain access to systems with shared accounts, the individuals who have access to these shared accounts are clearly identified within the SimpleConnect user interface and each user has a unique login ID.
R5.4: Change known default passwords, per Cyber Asset capability	SimpleConnect prompts the user to change the default admin account password and the account can be disabled.
R5.5: For password-only authentication for interactive user access, enforce strong passwords	SimpleConnect enforces strong passwords.
R5.6: For password-only authentication for interactive user access, enforce password changes every 15 months	SimpleConnect enforces password changes. The time frame in which password changes are enforced are configured by a SimpleConnect System Administrator.

R5.7: Limit number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts	SimpleConnect limits the number of unsuccessful authentication attempts. Once the limit is reached, the user account is locked. The number of unsuccessful attempts required to lock an account can be configured by a SimpleConnect System Administrator. Every authentication attempt, whether successful or failed, is logged. Authentication events are logged for both access to the SimpleConnect user interface, and for HIPswitch user authentication.
CIP-008-5: Incident Reporting and Response Planning	
R1: Cyber Security Incident Response Plan	The Tempered Networks solution can be an effective component of an Incident Response Plan (including Intelligent Islanding and on-demand secure network provisioning) by providing response mechanisms and procedures that are effective and easy to follow. This helps eliminate errors and omissions when exercising the response plan or responding to an actual incident.
R2: Cyber Security Incident Response Plan Implementation and Testing	
R3: Cyber Security Incident Response Plan Review, Update, and Communication	
CIP-009-5: Recovery Plans for BES Cyber Systems	
R1: Recovery Plan Specifications	The Tempered Networks solution can be an effective component of a Recovery Plan by providing recovery mechanisms and procedures that are effective and easy to follow. SimpleConnect enables authorized users to backup their configuration and quickly restore their configuration when necessary. This helps eliminate errors and omissions when exercising the recovery plan, and can increase the speed of recovery.
R2: Recovery Plan Implementation and Testing	SimpleConnect enables authorized users to backup their configuration and quickly restore their configuration when necessary.
R3: Recovery Plan Review, Update and Communication	
CIP-010-1: Configuration Change Management and Vulnerability Assessments	
R1: Configuration Change Management	The HIPswitch security appliances eliminate additional hosts that require configuration management.
R1.1: Develop baseline configurations	(Baseline configuration available in 2015)

R1.2: Authorize and document changes that deviate from existing baseline configurations	The Tempered Networks solution logs all network and remote access configuration changes.
R1.3: For changes that deviate from the baseline, update the baseline within 30 days	
R1.4: Verify changes against security controls in CIP-005 and CIP-007, verify, and document verification	
R1.5: Test deviations from baseline prior to implementation in production, and document the test results	The Tempered Networks solution facilitates the execution of testing deviations prior to implementation by providing isolated network environments in which the tests can be performed.
R2: Configuration Monitoring	Authorized users can monitor configuration changes via the SimpleConnect user interface, and log integration can generate alerts of configuration changes.
R3: Vulnerability Assessments	The Tempered Networks solution facilitates the execution of vulnerability assessments by providing isolated network environments within which the assessments can be performed.
CIP-011-1: Information Protection	
R1: Information Protection	The Tempered Networks solution facilitates information protection by providing encrypted communications channels between Cyber Assets. Even where Cyber Assets are using encrypted communications, the Tempered Networks solution provides an additional layer of security for these communications.
R2: BES Cyber Asset Reuse and Disposal	The Tempered Networks components feature a factory-reset capability that securely removes all configuration and cached data. Each retired HIPswitch can be further "revoked" from the SimpleConnect user interface in order to blacklist the unique cryptographic identity of the revoked HIPswitch.

Tempered Networks Value Proposition

The Tempered Networks solution is an independent layer of security that facilitates NERC CIP compliance and provides real and demonstrated security hardening, resilience and awareness. These benefits are achieved with minimal impact to operations, and HIPswitches can be deployed with only a short disruption in network connectivity. The Tempered Networks solution facilitates NERC CIP Compliance by:

1. Creating flexible Electronic Security Perimeters (ESPs) for distributed facilities and equipment
2. Providing secure, managed Access Points for connectivity to Cyber Assets within these ESPs
3. Centralizing governance, auditing, monitoring, logging, change control, and documentation of these Access Points and their associated configurations

4. Introducing overlays for individual user access (vs. shared access), user authentication, authorization, and auditing for remote access to Cyber Assets
5. Enabling ad-hoc networks for managing assets through test, patch, upgrade, remediate, and replacement phases

Next Steps and Call to Action

Best practices suggest comprehensive risk management, tied to a defense in depth cybersecurity implementation, is the appropriate approach for securing ICS. Network segmentation is a foundational building block of a defense in depth, layered security implementation. Standards from ISA are focusing on network segmentation because it can be used to minimize the connectivity for ICS to the absolute minimum, and protect that connectivity over shared network infrastructures. Additional standards from IETF and TCG (referenced below) show how these segmented networks can be efficiently managed at any scale.

The Tempered Networks solution is an implementation of industry standards that not only decouples and secures the ICS communications from a shared network, but also decouples the management of the ICS systems from the management of the shared network. This approach of delegated management makes it possible for an enterprise to deploy secure private networks as an internal service, while adding robust and flexible security to these critical systems.

Referenced Standards

North American Electric Reliability Corporation

- **Critical Infrastructure Protection (var)** – NERC CIP v3 (Subject to Enforcement) and v5 (Subject to Future Enforcement) [http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx]

International Society of Automation (ISA)

- **ISA TR 100.15.01 (2012)** - Backhaul Architecture Model: Secured Connectivity over Untrusted or Trusted Networks: [https://www.isa.org/store/products/product-detail/?productId=116759]

Trusted Computing Group (TCG)

- **TCG IF-MAP Binding for SOAP v2.1r15 (2012)** – IF-MAP for Network Security Coordination: [https://www.trustedcomputinggroup.org/resources/tnc_ifmap_binding_for_soap_specification]
- **TCG IF-MAP Metadata for ICS Security (2012)** – IF-MAP Metadata for Industrial Control Systems Security: [https://www.trustedcomputinggroup.org/resources/tnc_ifmap_metadata_for_ics_security]
- **TCG Architects Guide: ICS Security Using TNC Technology (2013)** – Whitepaper: [http://www.trustedcomputinggroup.org/resources/architects_guide_ics_security_using_tnc_technology]

Internet Engineering Task Force (IETF)

- **IETF RFC 5201 (2008)** – Host Identity Protocol Version 2 (HIPv2): [http://tools.ietf.org/html/rfc5201]
- **IETF draft-henderson-hip-vpls-06 (2013)** – HIP-based Virtual Private LAN Service (HIPLS): [http://tools.ietf.org/html/draft-henderson-hip-vpls-06]

To learn more, email sales@temperednetworks.com, call 206.452.5500, or visit temperednetworks.com.