

## **Requirements and Experience of Practical Secure Access Control and Management of Intelligent Systems**

|                       |                               |                           |
|-----------------------|-------------------------------|---------------------------|
| <u>Rodney Hughes*</u> | Siemens Australia (Ruggedcom) | rodney.hughes@siemens.com |
| Randy Carson          | Siemens Canada (Ruggedcom)    | randy.carson@siemens.com  |
| Alan Wang             | CSE-WArthurFisher             | alanw@cse-waf.co.nz       |

The intelligence of the power network, as well as any other domain, is undoubtedly increasing at exponential rates with the proliferation of all manner of new devices and applications relying on communication networks. It is increasingly common for asset owners to have an asset portfolio of tens, and even hundreds, of thousands of Intelligent Electronic Devices (IEDs). These IEDs represent the core of these new operational capabilities which in themselves introduce new dimensions to the engineering process as well as the maintenance of the operating systems. Device configuration, firmware updates and data retrieval forms the daily activities for any asset owner either directly and/or through an array of service providers.

Many new innovative solutions and operational practices are possible with these IEDs via both local and remote communication on the corporate WANs as well as dial-in, wifi and even bluetooth connections from an increasing range of fixed or portable smart user interfaces through to even smart phones/tablets.

In an environment where these IEDs have become a far more complex and integral part of the daily operation, asset owners generally will recognise the need for control of physical access to these systems in order to protect the integrity of these vital systems. Visitors would not be allowed to wander unimpeded through sites and even staff would have strict authorisations and procedures around what they can do on the site.

Clearly then the mere fact of these communication access to the IEDs introduces a new operational risk of cyber security of access control to these IEDs. It is a sad fact that in many installations IEDs are operating still with only the factory default password, if only for the sheer difficulty of maintaining those passwords as operational personnel join or leave the companies.

Cyber security systems must be introduced in an effective manner that enables, not hinders, the daily operations of the technical staff to access IEDs for activities such as:

- Asset condition monitoring,
- Event response and investigation,
- Maintenance (including vendor access),
- Control, protection and telecommunications engineering

Secure IED access requires password obfuscation at the IED itself as well as Role Based Access Control for staff, all which can be centrally managed, combined with automation of many of the routine and critical IED configuration and file management activities.

This paper reviews practical experience of the objectives, specifications and deployment of operational cyber security requirements for critical IED infrastructure.

## 1. THE MAJOR NEW RISK TO REAL TIME OPERATION

Cyber security is one of those terms that is bandied about in the assumption that everyone knows what that means and therefore with the presumption that things have already been put in place to provide effective measures thereto.

However that assumption and presumption are often found to be not true or limited in practical reality – many an electrical engineer would scoff at any suggestion of “restrictive” systems and procedures as, after all, *“anyone could climb the fence of an unmanned substation and press a button”*, or as the original Oceans 11 film of the 1960’s suggested, just *“blow up a few towers in the hills”*.

Modern utility networks and IEDs are under increasing security pressure. In the Global Risks 2012 Edition, the World Economic Forum lists cyber attacks in the top 5 risks in terms of likelihood. Trends enabling cyber security breaches include:

- Cloud computing approaches
- Increasing use of mobile devices
- Wireless technology
- Smart Grid deployment
- Worldwide remote access capabilities to remote machines and mobile applications
- The “internet of things”

In industrial security, vulnerability disclosures are headline news. Terms like ‘cyber attack’, SCADA system vulnerability’ and ‘hacking the grid’ are becoming headline news. Websites like SHODAN and ERIPP allow inexperienced hackers worldwide to find unprotected industrial devices exposed to the internet. Trends such as connection of automation networks with IT Networks and the internet for remote access, and increased use of open standards and PC based networks further amplify the opportunity for a security breach. Even when systems are considered secure and locked down there may be unforeseen factors that come into play – the recent “Heartbleed” bug in the OpenSSL software library is a good example of this.

The corporate security chain is only as strong as the weakest link. Security can fail at many points, including social engineering attacks, security of computer devices and network infrastructure, applications, and policies and guidelines. It is key to look at security from a holistic perspective, and create policies and guidelines that cover devices, systems, processes, and employees.

Whilst this particular paper is somewhat focused in regards to the electric power industry, communicating IEDs have become the core technology of all manner of industry domains covering all manner of sensors, controllers and systems. The principles here apply equally to:

- utilities: power, water, gas, telecommunications;
- transport control systems: road, rail, airport;
- mining and/or industrial plant;
- building/site management systems

and apply regardless of whether there is a centralised wide area SCADA system or just a localised automation system of some sort. Anywhere there are IEDs that are critical to the real time operation of the facility, access to the IEDs must be managed and controlled, and as

NERC CIP has recently been expanded, even regardless of whether there is internet connectivity to those IEDs.

In order to identify what is needed in terms of “**Secure Access Control and Management of Intelligent Systems**” as the subject of this paper, it is necessary to clarify:

- what exactly is an “Intelligent System” as Operational Technology and what has changed in recent times to demand this to be “Secure”; and
- what does it mean for staff to have “Access to” these systems; and
- what does it mean to have “Management of” these systems.

## **2. WHAT IS “OPERATIONAL TECHNOLOGY”**

Naturally we have all become highly familiar with Information technology (IT) applied in our daily business environment with main frames and PCs as the core infrastructure for the business processes and which are now intimately linked with internet access. As such we recognise the need for security around those systems to guard the essential intellectual property of the company.

Operation Technology (OT) is a more recent evolution of plant operational processes which rely on automatic communication mechanisms largely directly between the devices as well as some human access requirements. OT incorporates all the systems, devices and data that is used to operate and manage the asset owners facilities.

OT arguably started to appear in the 1980’s and 90’s with System Control And Data Acquisition (SCADA), or Distributed Control Systems (DCS) established over somewhat independent and largely proprietary communication systems. Whilst they have been subject of concerns in their own right, these early systems had “security by obscurity”, meaning the famous “air gap” with no physical communication path to other systems in the corporate environment. The Remote Terminal Units (RTU) have previously been the “end-point” of the communications network as they were connected to the rest of the facility by hundreds/thousands of wire based analogue signals or binary inputs/outputs – a communications network “air gap”.

Certainly SCADA type OT systems have become “connected” to the outside world with operators PCs sharing corporate LANs. However communications has continued to evolve and permeated into every facet of technology.

Just considering the electricity industry, since the late 1980’s, devices such as the protection relays have migrated to incorporate simple RS232, RS422, RS485 type communications as the RTU connection, eliminating thousands of wires in the facility. Initially these have been somewhat proprietary protocols but have moved to standards such as Modbus, DNP3, IEC 60870-5 etc and moreover have now also moved to full Ethernet TCP/IP based communications with arguably the most topical systems being IEC 61850.

Furthermore, now that the electric power industry has entered the infamous Smart Grid era, it is not just the protection relays that have some form of LAN connectivity. Indeed IEC 61850 points to all manner of sensors such as humidity, temperature, vibration, pressure, level, flow have data models under the T group Logical Nodes (LN) enabling more efficient engineering processes to enable the IEDs to communicate over the LAN.

## Requirements and Experience of Practical Secure Access Control and Management of Intelligent Systems

---

The result is a highly intelligent process operating as a “super-sized” connected system with a plethora of smart applications using a plethora of different IEDs and even connectivity via wide area wifi/radio based communication.

One particular distribution utility in Australia has identified that their asset base of IEDs will exceed 851 thousand devices by 2025 across a plethora of applications such as:

| Device                                  | Description   | Device                                   | Description  |
|---|---|--|--|
| SCADA RTUs                              | Controllers as part of the SCADA infrastructure             | Voltage Regulators (MV)                  | Cap bank solutions   |
| Terminal Server                         | Connection point for Serial Devices                         | Distribution Transformers                | Above and below ground   |
| Protection Relays                       | Primary network protection                                  | Distribution Regulators                  | Voltage regulating devices                                       |
| Reclosers                               | All reclosers in the network                                | Power Transformers                       | Primarily substations  |
| Fault Indicators (LFI,RMU, Fuse savers) | Attached to feeders   | Weather Stations                         | Environmental conditions   |
| Statistical meters                      | For monitoring of network power quality                     | Temp Sensors (Overhead)                  | Primarily remote temperature readings                            |
| Smart Revenue meters                    | For billing and near real time power quality (smart meters) | Underground Cable Monitoring             | Primarily remote temperature readings                            |
| Programmable Logic Controllers (PLCs)   | Controllers not directly associated with SCADA              | Embedded Generation (utility owned) GUSS | Grid level storage   |
| Substation Battery Charger              | Independent Device in Substation                            | Embedded Generation (utility owned) RUS  | Residential level storage  |
| Backup Generator Controller             | Independent Device in Substation                            | Embedded Generation (3rd party)          | Local Wind / Solar / Gas Turbine (around 5 MVA size)             |
| Main Generator Controller               | Remote power generation                                     | Electric Vehicle (EV) charging stations  | Charging stations that have grid control                         |
| Voltage Regulators (HV)                 | Standard StatVAR solutions                                  | Inverter Energy Systems                  | Primarily residential PV /battery systems that have grid control |

Scalability and reliability of any system designed to manage secure access across large networks is clearly important. As the number of devices under management grows, considerations must be made to ensure the system performance is not affected. Also, it is important to have scalable tools for maintenance of device and user information, bulk import capabilities, and a hierarchical method to view and access information.

Since this is a critical system, proper considerations need to be made to ensure very high reliability and uptime, especially during emergency situations where the utility will be relying heavily on the system. High availability, redundant, hot standby systems should be considered for the server, database, and network connectivity infrastructure. If this system is also obfuscating passwords of individual IEDs, a regular backup of IED passwords stored in an offsite location should be part of the operating procedures.

### 3. USER MANAGEMENT AND ROLE BASED ACCESS CONTROL

Remote access to IEDs has become a key operational requirement for any intelligent system, in many cases improving speed and accuracy of response to system events and failures. This requires a variety of personnel to be given suitable mechanisms and possibly varying controls at various stages of the system life cycle for that access for:

- engineering staff
- commissioning staff
- maintenance staff
- vendor support staff

#### 3.1. WHAT DOES INDIVIDUAL RBAC IMPLY

Role Based Access Control (RBAC) pertains to the concept of limiting the access to devices and device interaction based on the role of the individual. For example, a protection engineer

may only have access to protections devices, and may be further limited to a subset of the devices base on geographical location. The engineer may only have limited permissions on certain device types depending upon their role, and the secure access system should be capable of blocking not only access to certain login levels on a device, but specific commands in a Telnet session, for example. There are also scalability considerations at play here – the system should provide the capability to group users in roles and apply permissions at the group level. The most important role in any such system is the system administrator, this role has the ability to configure the rules and permissions for all users in the system.

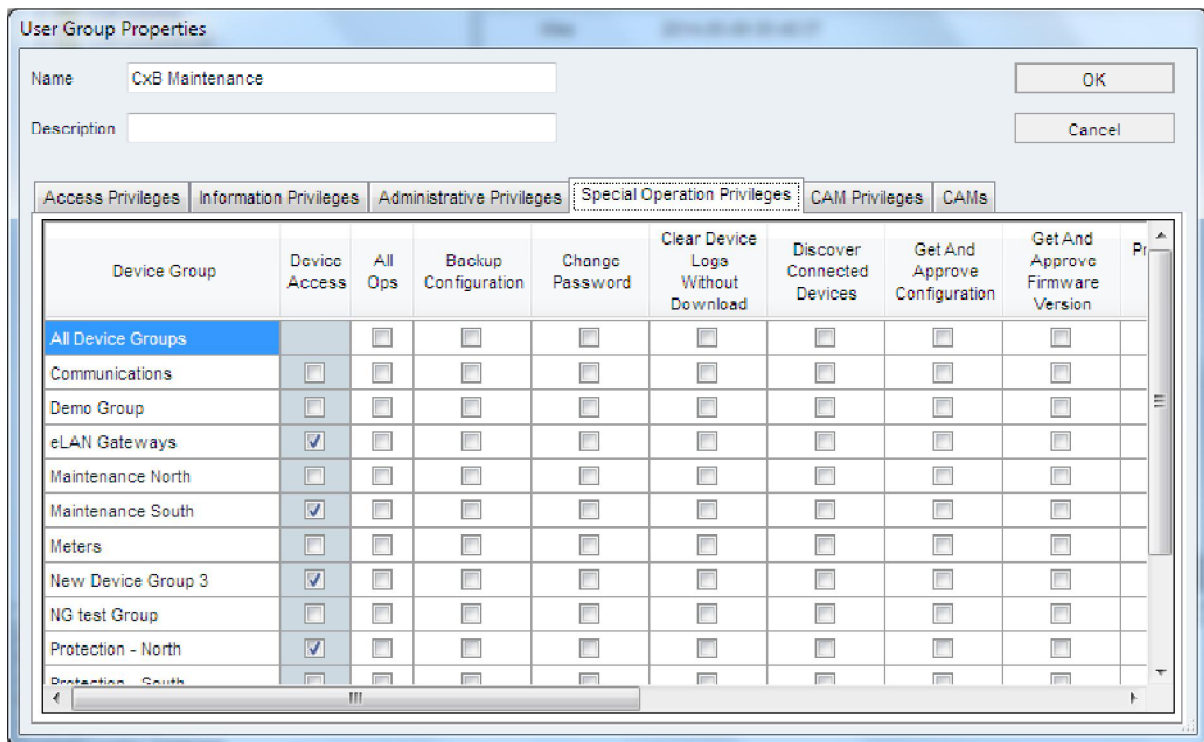


Figure 1 – Operational Privileges for a Given Role

A key concept in any secure remote access systems, such as the comprehensive Siemens Ruggedcom Crossbow solution, is IED password obfuscation. Individual IED passwords, network addresses, and even the network topology is not made available to the users of the system. The users may login to the system using corporate LDAP or radius credentials, and are then allow access to devices based on their role without having to know the individual IED passwords which are kept hidden within the remote access system. If an individual is no longer working for the company, once their credentials are removed from the corporate system they no longer have access to the system or the devices. This also allows for temporary access to be granted to service providers, contractors, or vendors who require access to specific devices. The system can also be setup to allow remote access via existing secure techniques such as VPN.

### 3.2. WHAT DOES NERC-CIP REQUIRE

Certainly the NERC CIP requirements are pushing organisations into new areas of governance, procedures and systems in the US. Whilst the same type of standard and legislation hasn't evolved in this region so much, as "good industry practice" they certainly become a reference of what we should be doing even in absence of legislation.

#### 3.2.1. USER ACCOUNT MANAGEMENT

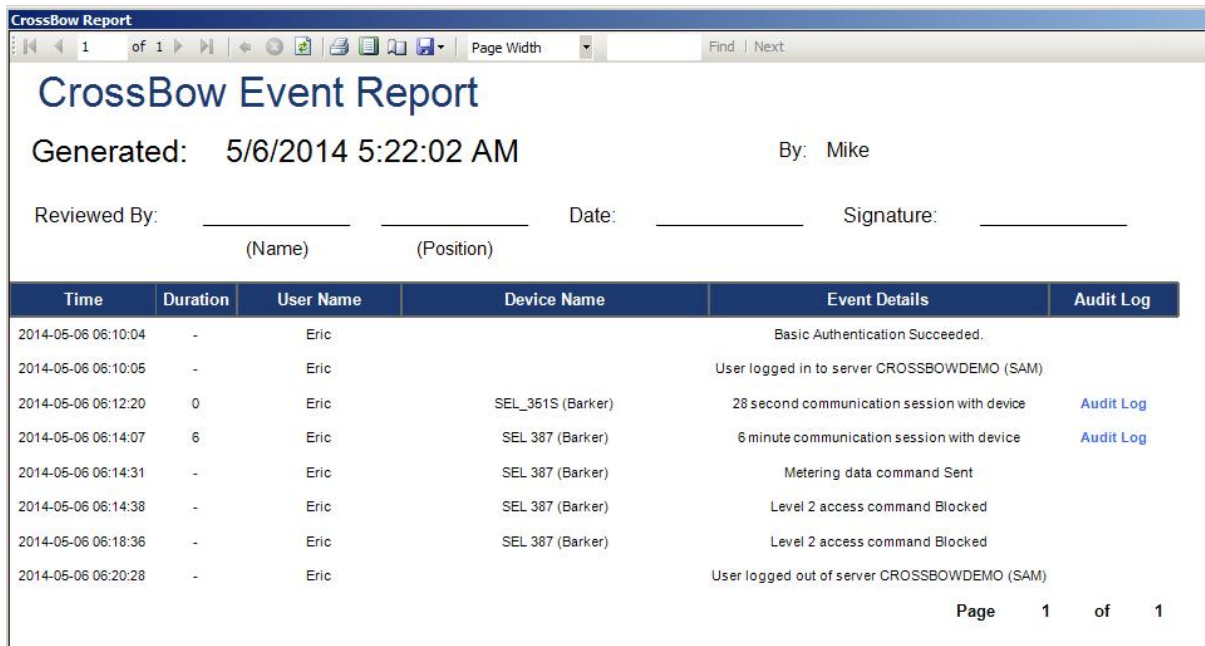
## Requirements and Experience of Practical Secure Access Control and Management of Intelligent Systems

CIP-004-3a R4.2 sets a 24 hour time limit to revoke access to assets when staff have been dismissed or have resigned, or seven days if they have no operational need for ongoing access. This requirement specifically demands a methodology to manage the ability of all types of personnel with potential remote access to the site and IEDs. Engineering staff, maintenance staff, condition monitoring staff, event response teams, and again as both direct asset owner employees, service providers, contractors and even vendor access.

Clearly it is impossible and extremely uneconomic to visit every remote site in 24 hours, sometimes even difficult to arrange work orders and staff to visit even one site to change access controls. Equally if the user has direct knowledge of any site/IED passwords, that knowledge cannot be erased. A central system that disables the user's log in at source is the only sensible solution as the Human Resources and Project Management procedures can take instant unilateral action. For a large utility with tens of thousands of connected IEDs the business case on this alone is potentially "millions of dollars" even in any one year.

### 3.2.2. USER ACTIVITY LOG (AUDIT TRAIL)

Another important consideration is logging of all activity and actions taken when connected to devices as outlined in CIP-005-3a R1. Timestamps of device connection by an individual user, and logging of commands sent and received from devices are invaluable if a forensic investigation of an activity is required. System activities must also be logged to provide an audit trail, such as addition and permission changes for users and groups, the running of key reports, password changes on IEDs, and system initiated actions such as retrieval of device configuration files and event files.



The screenshot shows a web browser window displaying a "CrossBow Event Report". The report title is "CrossBow Event Report" and it was generated on 5/6/2014 at 5:22:02 AM by Mike. There are fields for "Reviewed By" (Name and Position) and "Date" and "Signature". Below this is a table with the following data:

| Time                | Duration | User Name | Device Name       | Event Details                                | Audit Log                 |
|---------------------|----------|-----------|-------------------|--|---------------------------|
| 2014-05-06 06:10:04 | -        | Eric      |                   | Basic Authentication Succeeded.              |                           |
| 2014-05-06 06:10:05 | -        | Eric      |                   | User logged in to server CROSSBOWDEMO (SAM)  |                           |
| 2014-05-06 06:12:20 | 0        | Eric      | SEL_361S (Barker) | 28 second communication session with device  | <a href="#">Audit Log</a> |
| 2014-05-06 06:14:07 | 6        | Eric      | SEL 387 (Barker)  | 6 minute communication session with device   | <a href="#">Audit Log</a> |
| 2014-05-06 06:14:31 | -        | Eric      | SEL 387 (Barker)  | Metering data command Sent                   |                           |
| 2014-05-06 06:14:38 | -        | Eric      | SEL 387 (Barker)  | Level 2 access command Blocked               |                           |
| 2014-05-06 06:18:36 | -        | Eric      | SEL 387 (Barker)  | Level 2 access command Blocked               |                           |
| 2014-05-06 06:20:28 | -        | Eric      |                   | User logged out of server CROSSBOWDEMO (SAM) |                           |

Page 1 of 1

Figure 2 – Example of Activity Audit Report

## 4. IED SYSTEM MANAGEMENT

As is evident from the IED count example in the earlier section, it is exceedingly impractical to manage individual IED passwords by manual processes, particularly when staff join/leave the access groups. A core requirement is therefore a system which is both centrally managed and centrally accessed.

### 4.1. WHAT DOES NERC-CIP REQUIRE?

CIP -003-3 sets out the requirements to be able to identify when there are changes to the devices as both hardware and software issues. This directly requires monitoring for both

- IED Firmware version
- IED Configuration version and setting changes

Whilst we generally don't see "random" changes in either of these, devices are replaced from time to time in the field, even upgraded in some way, or settings may be changed/applied in the field. There may be policies, if not preferences around how much of those changes may be permitted "over the wire".

However even if they are done directly on site, they need to be logged, reported and verified as being valid and anticipated changes that don't represent a direct security breach of the system, or present a risk to overall grid performance and security. Taking this to the next logical requirement is to provide an alert system by email or mobile phone text alert to specific staff about the particular version change.

#### **4.2. IED PROPRIETARY COMMAND SYSTEM INTEGRATION**

Many IED vendors have proprietary client software used to configure and monitor their devices. Alternatively, some devices use simple HTTP or Telnet/SSH sessions for control and configuration. It is important for any secure remote access system to allow transparent use of these client software options for IED access. However, the secure remote access system, such as the Siemens Ruggedcom Crossbow solution, must be capable of logging not only access, but also what commands and functions are performed. When fully integrated into the RBAC, the system can also be used to block specific commands based on the user's role and privileges.

#### **4.3. OPERATIONAL RECORDS RETRIEVAL**

Another challenge for utilities today is retrieval of records and information from IEDs. As networks become more intelligent, much more information is produced and needs to be effectively managed. Fault, sequence of events, and oscillography files are all examples of records that are highly desirable to have available and searchable. A secure remote access system can perform automated tasks to login and retrieve this data from IEDs, and catalogue and store it in a secure database for future analysis.

#### **5. RELIANCE ON COMMUNICATION PATH AND WHAT IF IT FAILS**

A secure remote access system typically bridges the utility's IT network (clients for end-user access, servers, database), and the secure operational network (substation gateways and IEDs). This type of architecture can be made highly secure: user authentication, servers and databases can be centralized in a secure facility, and certificate based authentication and encryption can secure the data path between the central facility and the remote locations.

The weak link in this type of architecture is the communication path to the remote devices. If this path is interrupted, local personnel may not be able to access IEDs if the IED passwords are managed by the central server. While it may be possible for the local personnel to call the central facility to obtain a password, this poses a security risk. A more desirable solution is for the system to maintain a copy of the database specific to that location for situations when communication is lost. The local controller and database can log all activity during the communication outage, and synchronise back up with the central system once the communication path is restored.

## 6. CONCLUSION

Cyber security seems to be something that most people recognise as fundamental and essential concepts. In many cases the practical implementation of mechanisms, and in some cases even the governance procedures, to enforce and manage cyber security as far as remote access to critical Operational Technology environments are often left to somewhat rudimentary reliance on a firewall.

However the issues associated with day-to-day operation of a system of IEDs demands a far more comprehensive array of controls in particular due to the proliferation of devices that are associated with remote access, as well as the proliferation of different types and numbers of users requiring access of different levels.

As electrical power networks become more intelligent and automated, transmission and distribution utilities are implementing secure remote access systems to manage these networks in a secure, reliable way. Globally, many utilities have thousands of IEDs managed by these systems. Initially deployed for secure remote access, these systems are being used to reduce truck rolls to remote devices, and to manage compliance to NERC CIP5 requirements

This paper sets out the requirements for a secure approach to remote access in any industry as:

- Resilient central and remote architecture
- Centrally managed Users
- Comprehensive user-specific RBAC mechanisms
- Centrally accessed with IED password obfuscation
- IED-type agnostic operation
- Enhanced management of 'integrated' IED

## 7. REFERENCES

Gartner, Inc "IT and Operational Technology: Convergence, Alignment and Integration"  
<http://www.gartner.com/newsroom/id/1590814>

United States Nuclear Regulatory Commission "Cyber Security in Digital Instrumentation and Controls" <http://www.nrc.gov/about-nrc/regulatory/research/digital/key-issues/cyber-security.html>

CIGRÉ Technical Brochure 419 "Treatment of Information Security for Electric Power Utilities" <http://www.e-cigre.org/> (Individual CIGRE Members or staff of CIGRE Member companies can download PDF for free using the Membership number login)

CIGRÉ Technical Brochure 427 "Impact of Implementing Cyber Security Requirements using IEC 61850" <http://www.e-cigre.org/> (Individual CIGRE Members or staff of CIGRE Member companies can download PDF for free using the Membership number login)

CIGRÉ Study Committee B5, Session proceedings 2012, Preferential Subject 2: "Utilization and Application of Remote Access for Protection and Automation Systems", 11 Papers and 38 Contributions



## 8. APPENDIX: NERC CIP STRUCTURE

### Subject to Enforcement

|            |  |
|------------|--|
| CIP-002-3  | Critical Cyber Asset Identification        |
| CIP-003-3  | Security Management Controls               |
| CIP-004-3a | Personnel & Training                       |
| CIP-005-3a | Electronic Security Perimeter(s)           |
| CIP-006-3c | Physical Security of Critical Cyber Assets |
| CIP-007-3a | Systems Security Management                |
| CIP-008-3  | Incident Reporting and Response Planning   |
| CIP-009-3  | Recovery Plans for Critical Cyber Assets   |

### Future Enforcement

|             |   |
|-------------|---|
| CIP-002-5.1 | BES Cyber System Categorization                               |
| CIP-003-5   | Security Management Controls                                  |
| CIP-004-5.1 | Personnel & Training  |
| CIP-005-5   | Electronic Security Perimeter(s)                              |
| CIP-006-5   | Physical Security of BES Cyber Systems                        |
| CIP-007-5   | System Security Management                                    |
| CIP-008-5   | Incident Reporting and Response Planning                      |
| CIP-009-5   | Recovery Plans for BES Cyber Systems                          |
| CIP-010-1   | Configuration Change Management and Vulnerability Assessments |
| CIP-011-1   | Information Protection  |

## 9. APPENDIX: NERC CIP EXTRACTS

### CIP -003-3 Security Management Controls

R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

CIP-004-3a R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

CIP-005-3a R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

#### **10. AUTHOR BIOGRAPHIES**

Rod Hughes has over 33 years' experience in the power industry across New Zealand, Australia and internationally specifically involved in protective relay, instrumentation and metering solutions. He is recognised as a thought leader in deployment and management of intelligent systems and is one of the longest serving members of the CIGRE Australia B5 Panel, including winning two Merit Awards. He is always keen to assist the industry at large, and is a prolific contributor to protection and IEC 61850 forums on LinkedIn. He has served in senior management roles with a vendor (including France for three years), utility and consulting firms including his own private consulting focused on IEC 61850 deployment and change management advisory along with vendor-agnostic training services. He is now also the Business Development Manager for Siemens Ruggedcom responsible for support of network solutions for the power industry.

Randy Carson has 29 years experience in the telecom and electrical utility industry in Canada. He is currently Senior Product Manager for the Rugged Solutions software portfolio at Siemens RuggedCom. His interests span across data and IP communications and networking, including remote access and automation.

Alan Wang received his BE and ME (Honours) in Electrical and Electronic Engineering from the University of Auckland, New Zealand. He has been with CSE-W.Arthur Fisher Ltd since 2011 and is currently in the Smart Grid Solutions Group and representing Siemens Ruggedcom - Industrial Hardened Networks products in New Zealand. He has particular interest towards technologies in the power system industry and substation automations & communications.