PNNL-26729

Pacific Northwest NATIONAL LABORATORY

Proudly Operated by Battelle Since 1965

Secure ICCP

Final Report

June 2017

M.J. Rice
C.A. Bonebrake
G.K. Dayley
L.J. Becker

U.S. DEPARTMENT OF ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

**Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov**

**Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
email: orders@ntis.gov <http://www.ntis.gov/about/form.aspx>
Online ordering: http://www.ntis.gov**

This document was printed on recycled paper.
(8/2010)

PNNL-26729

Secure ICCP

M.J. Rice
G.K. Dayley
C.A. Bonebrake
L.J Becker

June 2017

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99352

Acronyms and Abbreviations

CEDS	Cybersecurity for Energy Delivery Systems
CISCO	CISCO Systems
COTS	consumer off the shelf
DEWG	Data Exchange Working Group
EIOC	Electricity Infrastructure Operations Center
EMS	Electronic Message System
ICCP	Inter-Control Center Communications Protocol
IP	internet protocol
IPP	Independent Power Producers
ISO	Independent System Operators
MACE	MMS Application Certificate Exchange
MMS	Manufacturing Message Specification
NUG	Non-Utility Generators
OAG	Open application Group
PNNL	Pacific Northwest National Laboratory
RC	Reliability Coordinator
RTO	Regional Transmission Operators
SCADA	Supervisory Control and Data Acquisition
SISCO	Systems Integration Specialists Company
SSL	Secure Socket Layer
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WECC	Western Electricity Coordinating Council
WON	WECC Operational Network

Contents

Figures

1.0 Introduction

Inter-Control Center Communications Protocol (ICCP), defined by the IEC 60870-6 TASE.2 standard, was developed to enable data exchange over wide area networks between electric system entities, including utility control centers, Independent System Operators (ISOs), Regional Transmission Operators (RTOs) and Independent Power Producers (IPP) also known as Non-Utility Generators (NUG). ICCP is an unprotected protocol, and as a result is vulnerable to such actions as integrity violation, interception or alteration, spoofing, and eavesdropping. Because of these vulnerabilities with unprotected ICCP communication, security enhancements, referred to as Secure ICCP, have been added and are included in the ICCP products that utilities have received since 2003 when the standard was defined. This has resulted in an ICCP product whose communication can be encrypted and authenticated to address these vulnerabilities.

2.0 Background

The plan for this task was that the Pacific Northwest National Laboratory (PNNL) team would observe participating utilities as they worked through the business policies and processes to turn on Secure ICCP, noting where challenges arise and aiding the utilities in reducing those challenges. However, when this project was shared with participants at the February 2013 Western Electricity Coordinating Council (WECC) Data Exchange Working Group (DEWG) meeting, it was proposed by one of the DEWG members that the Pacific Northwest National Laboratory (PNNL) Electricity Infrastructure Operations Center (EIOC) be leveraged. This proposal resulted in focusing the effort to work with Peak Reliability to establish an ICCP link between Peak Reliability and the PNNL EIOC. This will be one of the first steps in this CEDS task as we work to facilitate the rollout by electric utilities of Secure ICCP products. This DOE-funded project involves PNNL working with WECC-member utilities (who have expressed interest in participating), Peak Reliability, and Alstom Grid to turn on Secure ICCP associations at strategic, select existing installations in order to better understand some of the potential barriers to organizations in using Secure ICCP.

The major stumbling block for utilities in turning on secure ICCP is difficulties with availability or interoperability with other utilities. Every device on the network needs a number of certificates to communicate with another entity. This creates a logistical hurdle to overcome, each device needing several certificates is not a hard problem but when multiplied by many nodes in each utility it quickly becomes hard to manage and implement. While secure once implemented a less complex implementation would see more adoption even if security was not as strong.

3.0 Overview of Configuration

3.1 ICCP

When two EMS systems need to exchange data, the ICCP engineers enter the information about ICCP link into the software. In the Western United States interconnection this is done by using a standard form that an ICCP engineer will fill out to give to the other entity information about his ICCP server. This forms specify the data needed and the locations that they need to flow from and to. The forms used go through significant scrutiny to make sure the right amount of data is exchanged and that each party really needs the data requested. The approval process for these agreements can take a long time or can happen quickly, the latter being the usual case for a renewal.

The information in these forms include IP Addresses, AR Names, Data Points, transmission frequencies, and other information that is sensitive to the utilities and is important to protect for cyber security reasons. Much care and details goes into putting these forms together as it drives the system configurations to make ICCP run.

3.1.1 Setting up the SISCO Stack

SISCO ICCP stack is the most common network stack used for implementing ICCP in an EMS. The stack handles the ICCP checks, such as AR name validation, and leaves the data management to the EMS software. This common stack also helps insure interoperability across the different vendors. This common stack also makes implementation easier as both parties can work through a common tool to identify lower level connectivity problems on a new connection.

3.1.2 Setting up the OAG

Each vendor has different interfaces to build a configuration for the ICCP data exchanges. Our system is an Alstom EMS using e-terracomm to handle our connections. Configuring our system includes tasks to configure the machine level connections, then the configuration of the data items being passed, like is the data outbound or inbound. After the model is built and validated, the model has to be deployed to the running system. Once both sites have completed this, then the link is turned on and the connection is made.

Companies may also have to run the configuration changes through a configuration board and a change management system before deploying to the running system. These additional steps can lengthen the time needed to deploy a new ICCP link or update an existing one. The steps PNNL went through with our partners can be found in Appendix B.

3.2 Secure ICCP

3.2.1 Overview of Securing ICCP traffic

Non secure ICCP traffic is transmitted in such a way that an adversary using a network analyzer such as Wireshark would be able to see the data in plain text. The network analyzer is able to capture internet protocol (IP) packets that are sent across the network. These IP packets have a known format containing things such as the header, the destination address, and the payload. The payload in an ICCP packet is sent clear text and can be read by anything device on the network.

Secure ICCP packets are formed in the same format as non-secure ICCP packets. However the biggest difference is in the payload. That payload is encrypted using the certificates installed on the ICCP server. This provides a server on the receiving end a way to verify the data and its integrity.

3.2.2 Selecting or Creating a Certificate Server

In order to move to a secure ICCP connection, a certificate server is required. This system has to be placed so that all entities that are going to use secure ICCP can access it for certificate validation. Setting up this server and establishing the root certificates is an import step to enable certificate management for encryption.

3.2.3 Generating Certificates

The certificate server owner will need to get the information for the ICCP server(s) to generate the machine specific certificates. Each server needs 4 certificates to start, and then 2 certificates on each update cycle. 2 certificates are for the MACE security and 2 certificates are for the encryption security. Once the certificates are generated, the public keys have to be installed on the server(s) that are participating in the secure configuration.

3.2.4 Setting up the SISCO Stack

The SISCO stack has to be updated to allow secure ICCP. Once the upgrade is complete, the certificates have to be added into the stack configuration. The addition of the certificates and the configuration of the stack will allow the stack to make a secure connection. If a secure connection fails, the connection stops and goes into an error state. The stack can also be configured to fail back to an unsecure connection to keep a connection alive.

3.2.5 Setting up the OAG

Vendor implementation can vary, but for Alstom, the configuration change was only a few steps. The connection level configuration needed a check box to allow secure connection and the check box for unsecure fallback was available (set based on configuration needs) for checking. Validate the change and deploy the updated model. The interconnected configurations setups needed to operate a secure ICCP link are in figure 1.

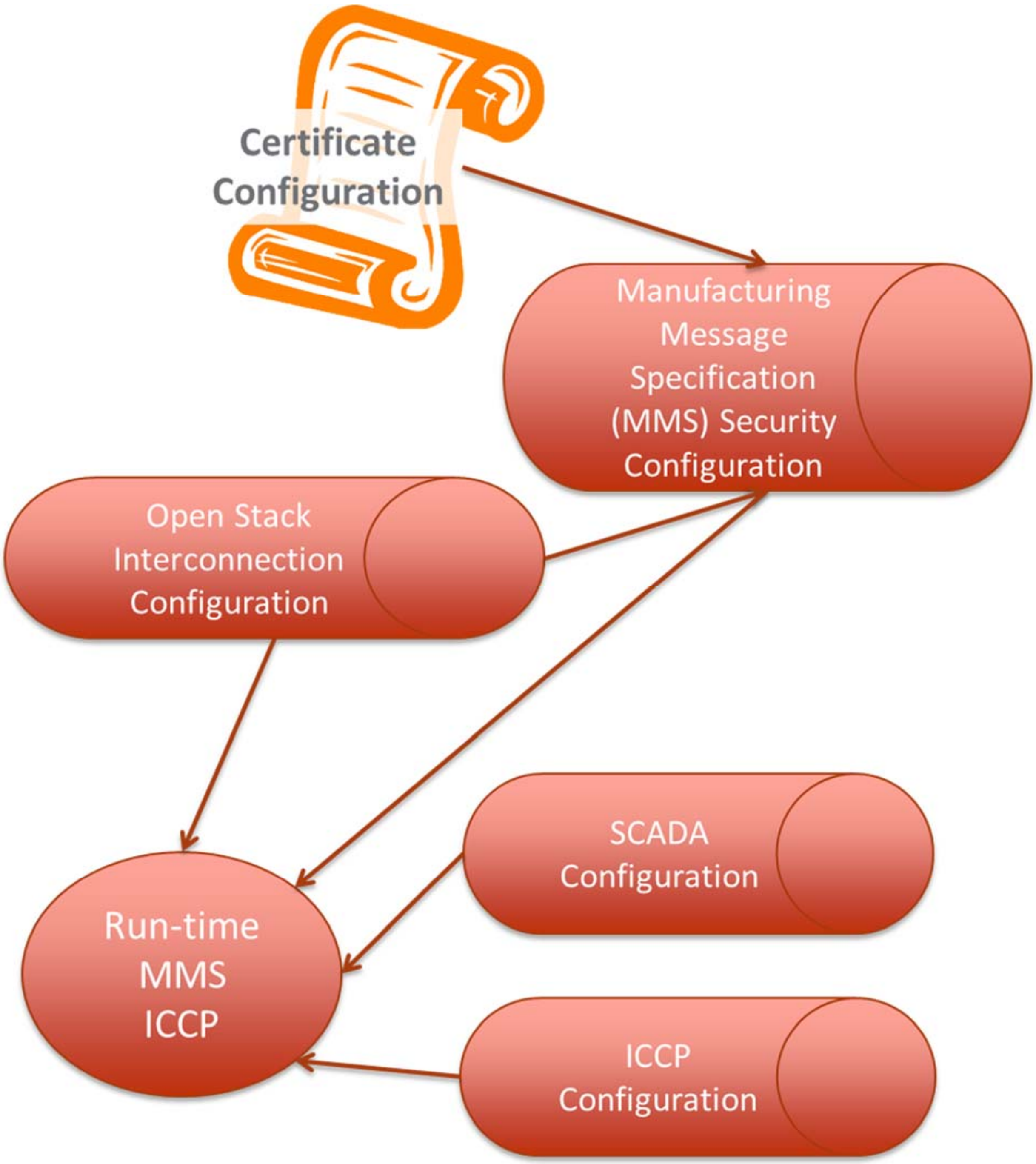


Figure 1Configuration of Secure ICCP

4.0 Accomplishments

Before any ICCP links with utilities could be made, PNNL needed access to the WECC Operational Network (WON). This required a dedicated AT&T link to the WON with approvals and physical connections. This process took much longer than expected, PNNL began attempting to establish a connection to the WON in March 2014 and did not have connection until August 2014.

PNNL contains a full Alstom EMS located in the Electricity Infrastructure Operations Center (EIOC), which was used to successfully create both a standard ICCP connection and secure ICCP connection internally. The redundant system was separated into two independent systems and setup to communicate through a firewall from separate VLANs to represent a prototypical network infrastructure between two interties. The high level architecture is illustrated in Figure 2.

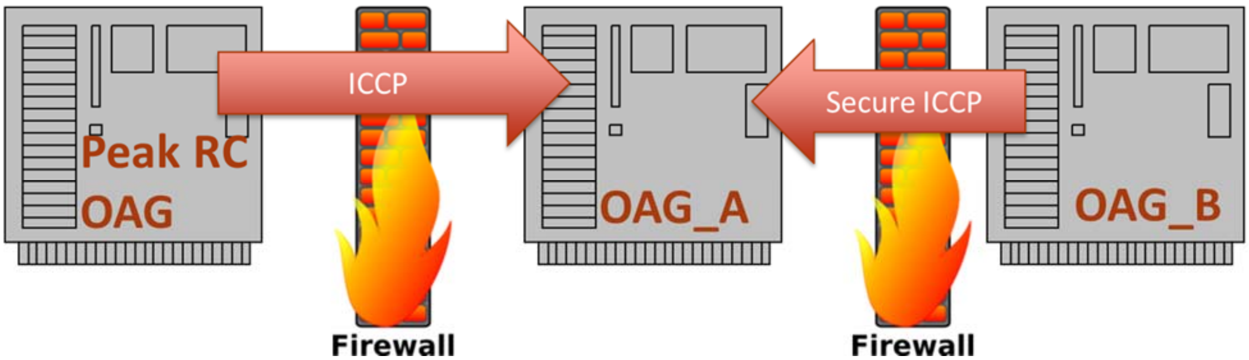


Figure 2 Logical Connections between OAG_A (system under test) and other OAG Boxes connected in the project

As a first step, PNNL internally created a secure ICCP link between the two independent systems. This task was more difficult than the initial ICCP connection. Extra components needed to be installed and modifications made to enable secure ICCP features. A key server also needed to be created and appropriate certificates generated and distributed to use with secure ICCP. After some trial and error and some assistance from Alstom, a secure ICCP link was created and data passed. PNNL demonstrated standard and secure ICCP connections working to Ryan Egidi on September 11, 2015. This the connection on the right side of Figure 2 where OAG_A is receiving data from OAG_B. The screen captures in Figure 3 show the different states of secure ICCP note. There is nothing alarming or easily identifiable of the system operating without security enabled. The change in the display that informs the user communication channel has failed to established secure connection is the words “MACE” and “SSL” change from black text to red text.

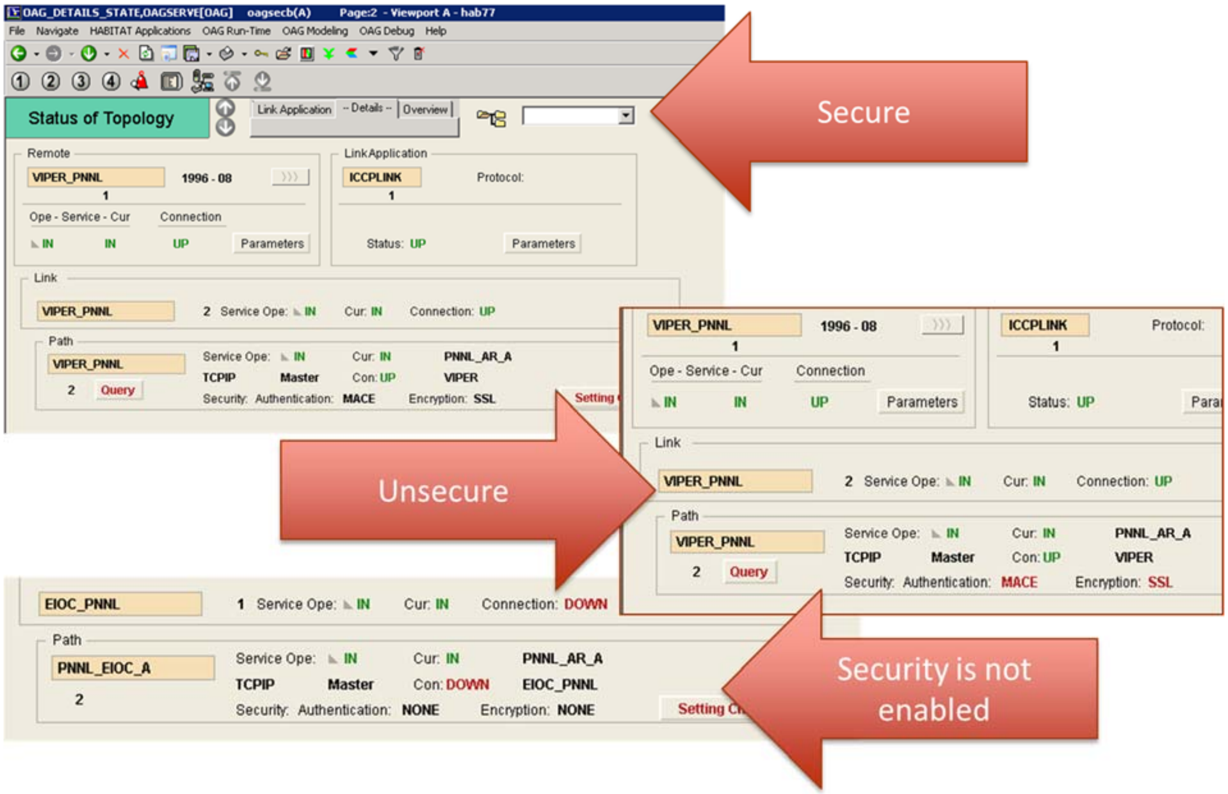


Figure 3 Screens captures of secure ICCP and different modes of operation: Secure, Unsecure, and Security not enabled

PNNL worked with Peak RC to establish a secure ICCP link. PNNL had a successful connection with Peak RC via ICCP in October 2014. This initial connection shows that a good ICCP link was created between PNNL and Peak RC providing the path towards the implementation of secure ICCP. This the connection of OAG_A receiving data from Peak RC OAG (Figure 4).

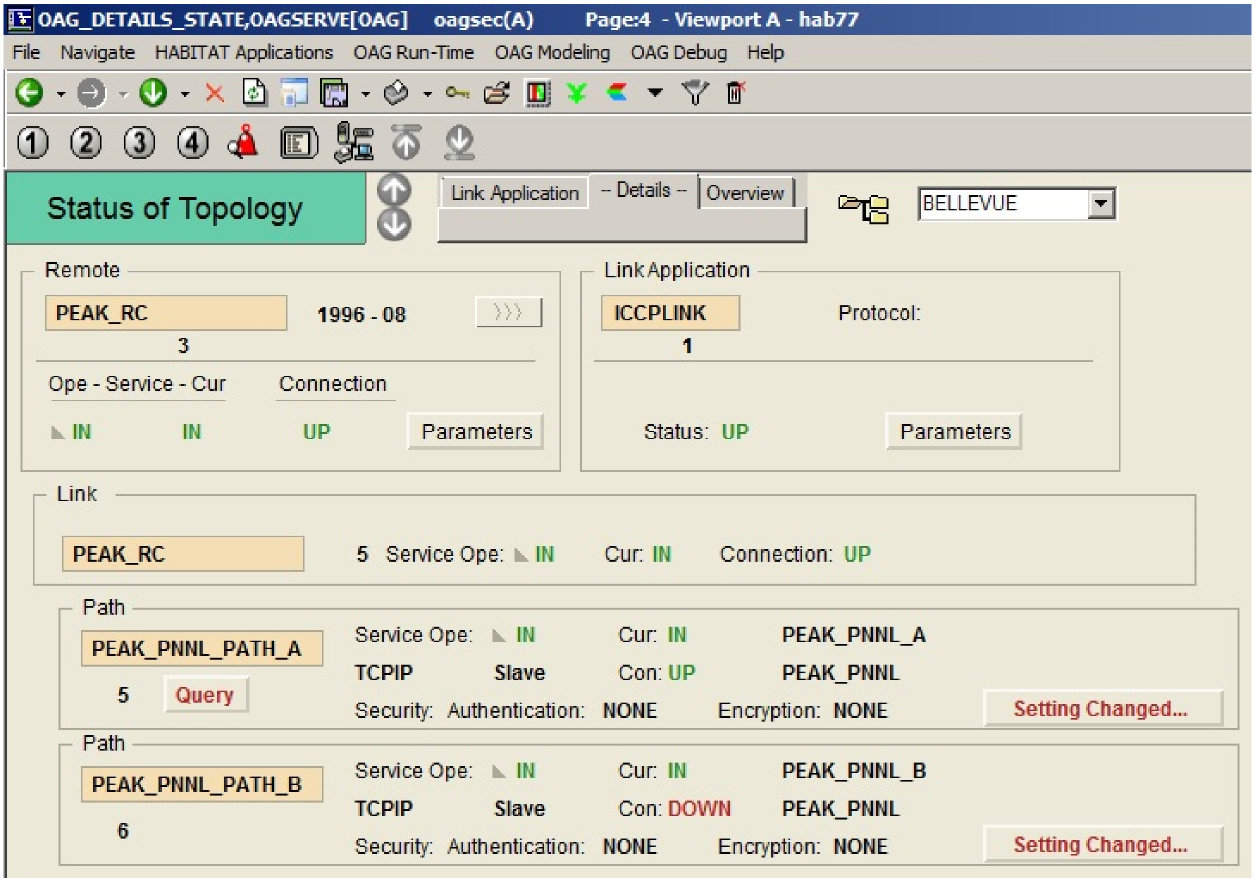


Figure 4 Screen capture of PNNL receiving data from Peak RC

When attempting to implement secure connection with Peak RC several issues arose. Peak RC needed to install more components; this caused an issue with the system and required a rebuild of the system to complete. In the end, a secure ICCP connection between PNNL and Peak RC was not feasible for various reasons including limited staff availability.

Awareness of the project activities have been shared with the community through participation in the DEWG meetings. While it is common for there to be ICCP links between utilities, secure ICCP is rarely implemented if at all. It is more common for ICCP links to be made through secure links (e.g., VPN tunnels).

5.0 Technical Difficulties

While ICCP is commonly used, secure ICCP is not. This means that there is limited experience, documentation and user community to support it. Secure ICCP is stated as functional by software manufacturers, but actual implementation and results may vary due to lack of use and continual testing throughout product life cycles. Differing configurations and versions between utilities can also create different experiences with respect to implementation (e.g., the installation of patches and software components).

Having support from the EMS manufacturer allowed PNNL to implement secure ICCP, but not without faults. Given the complex nature of an EMS, not all configurations are going to be identical; and therefore, are not always going to be implemented with the same level of effort.

When converting from an existing system using normal ICCP, there are components missing that would be required to implement secure ICCP. There are updates to both the SISCO stack and the ICCP server (Alstom OAG in this case) that need to be installed and configured. It was discovered that installing the secure ICCP components on an existing ICCP server can cause the system to be broken and a fresh install required.

The experiences and implementations performed for this test were all using Alstom EMS software. It is uncertain how this experience and level of effort would have differed with other brands of EMS software.

6.0 Other Difficulties

Other than the technical issues with software installation and configuration, there were some other difficulties. There were some issues with resources and priority related to this specific effort. While both PNNL and Peak RC worked well together and had a good relationship, immediate operational priorities trumped the implementation of a non-critical system (creating this secure ICCP link).

The connection to the WON was also not without its problems. It took 6 months to get the AT&T link to the WON. PNNL is not sure if this typical time to establish a connection to the WON, but did produce significant delays in the implementation of an ICCP connection to Peak RC.

A potential difficulty can be the coordination and agreement on a certificate authority. For this test, we setup a dedicated key server at PNNL in the EIOC to generate and validate certificates. In practice, a certified certificate authority may be desired. Once a certificate authority is defined, it was discovered that the secure ICCP implementation created for this test had a particular configuration for certificates that can cause issues if not requested and generated with the correct settings. There are a lot of certificates to keep track of as each secure ICCP server requires three certificates. Peak RC has ICCP connections with 20 plus entities, and with 4 ICCP servers per entity an approximate number of certificates would be 240 for all external connections.

It may be difficult to make a business case for the implementation and use of secure ICCP as there is already a work around that gets the job done without repercussions of insecure data and regulatory fines. Typical non-secure ICCP can be sent through secure connections that require less work to maintain (fewer certificates, dedicated systems without complex software, etc.).

7.0 Lessons Learned

Throughout this project, several things were learned. Secure ICCP isn't a new standard and isn't new to software manufacturers, which makes for consumer off the shelf (COTS) products. Even though ICCP is widely used, secure ICCP is not, leading to a lack of experience and knowledge of implementation. There currently is not a known driver for the implementation of secure ICCP, especially when other methods exists and are commonly used for more than just ICCP traffic/links.

For this case, a connection to a dedicated network is required. Obtaining that connection turned out to be a long process and caused significant delays in the progress of the project. What should have been a simple task turned out to be a drawn out and painful process. That being said, this should only be done once to establish the connection and shouldn't be a continued setback.

Even with COTS software that already had secure ICCP as a feature, the actual implementation was not as easy as hoped. Creating the environment took longer than expected with the various components that needed to be installed and configured along with the limited experience leading to some trial and error. Documentation existed, but that doesn't mean that it isn't without inconsistencies or faults, especially for a feature that is rarely used if at all. Luckily, Alstom was available to assist with providing additional information and details as we worked through the process.

Coordinating between a national lab and a utility, both with limited staffing, made for difficulties in finding time when both parties were available. Due to the unforeseen delays, time became increasingly difficult to coordinate as the project progressed. In the end, the investment of resources to implement secure ICCP became too great to justify its completion. The Peak RC test system was broken in the process and a bug report was issued to Alstom.

8.0 Conclusion

It was proven that a secure ICCP link can be created using off the shelf components. Like many large and complex software implementations, it should be expected that there will be difficulties and delays, but once the first instantiation of secure ICCP is created, all subsequent links will be made easier through experience and having the correct infrastructure installed. The hurdles weren't great, but were time consuming.

Secure ICCP is perfectly functional, and when correctly implemented, works well. However, without a good driver and business reason, it is difficult to justify making the change to secure ICCP from the existing systems that work at securely passing data using standard ICCP.

Appendix A

CISCO Stack and Certificates

Run "osill2.exe"
Menu: Configuration → Network → Addressing…

1. Hosts Tab
   1.1. If not present, add new host
      1.1.1. Host Name = localhost
      1.1.2. IP Address = XXX.Y.Y.Z
      1.1.3. Check the checkbox "local"
         1.1.3.1. Make sure this is the only host that is checked local
   1.2. Add new host
      1.2.1. Host Name = PEAK_PNNL_AA
      1.2.2. IP Address = XX.YYY.ZZ.193
   1.3. Add new host
      1.3.1. Host Name = PEAK_PNNL_BB
      1.3.2. IP Address = XX.YYY.ZZ.194
2. AR Names Tab
   2.1. Add new record
      2.1.1. AR Name = PEAK_PNNL_A
      2.1.2. Host Name = PEAK_PNNL_AA
      2.1.3. AP Title = 2 16 3826 84 69 77 83 49 73
      2.1.4. PSEL = 0000 0001
      2.1.5. SSEL = 00 01
      2.1.6. TSEL = 00 01
      2.1.7. AE Qualifier = 2
      2.1.8. Shared Locally = checked
   2.2. Add new record
      2.2.1. AR Name = PEAK_PNNL_B
      2.2.2. Host Name = PEAK_PNNL_BB
      2.2.3. AP Title = 2 16 3826 84 69 77 83 50 73
      2.2.4. PSEL = 0000 0001
      2.2.5. SSEL = 00 01
      2.2.6. TSEL = 00 01
      2.2.7. AE Qualifier = 2
      2.2.8. Shared Locally = checked
   2.3. Add new record
      2.3.1. AR Name = PNNL_AR_A (or use value recorded above)

2.3.2. Host Name = localhost
2.3.3. AP Title = 2 16 3826 80 78 78 76 49 73
2.3.4. PSEL = 0000 0001
2.3.5. SSEL = 00 01
2.3.6. TSEL = 00 01
2.3.7. AE Qualifier = 1
2.3.8. Shared Locally = checked

Adding Secure Configuration:

Appendix B

Alstom OAG

Environment Variables

Check for environment variable “LOCAL_AR”

Record value: ___________________________________

Or

Set (OAG-A):
    LOCAL_AR=PNNL_AR_A
Set (OAG-B):
    LOCAL_AR=PNNL_AR_B

OAG Modeling

Link Applications

ICCPLINK:
- Flow Control
  - T1 = 60
  - T2 = 30
- Queue Timer
  - T1 = 50
  - T2 = 100
- Statistic Timer = 60
  - Staggering Timer = 1
- Queue Max
  - Size = 90
  - Resources = 4

Under the ICCPLINK application:
Add new TCP AR Name Record:
    PNNL_AR_A or PNNL_AR_B

Topology

1. Add new Remote Record
   1.1. Name = PEAK_RC
   1.2. Type = ICCPLINK
   1.3. In Service = checked

1.4. Remote Domain = PNNL_PEAK
1.5. Version = 1996
1.6. Bilateral Table ID = 1
1.7. Max Scan Rate = 10
2. Add new Link Record
2.1. Name = PEAK_RC
2.2. Retry Timeout = 30
2.3. In Service = checked
3. Add new Path Record
3.1. Name = PEAK_PNNL_PATH_A
3.2. In Service = checked
3.3. Remote AR Name = PEAK_PNNL_A
3.4. Local = 1
3.5. Domain Name = PEAK_PNNL
3.6. Master = checked
4. Add new Path Record
4.1. Name = PEAK_PNNL_PATH_B
4.2. In Service = checked
4.3. Remote AR Name = PEAK_PNNL_B
4.4. Local = 1
4.5. Domain Name = PEAK_PNNL
4.6. Master = checked

DATA ITEMS → TYPE
Add 17 Data Items (numbers 161 – 177)

Name	Base Type	Qual	TS	MS	Cov
W087_A001638	REAL32	Checked	Unchecked	Unchecked	Unchecked
W087_A001640	REAL32	Checked	Unchecked	Unchecked	Unchecked
W087_A001641	REAL32	Checked	Unchecked	Unchecked	Unchecked
W087_A001643	REAL32	Checked	Unchecked	Unchecked	Unchecked
W087_A001646	REAL32	Checked	Unchecked	Unchecked	Unchecked
W087_A001614	REAL32	Checked	Unchecked	Unchecked	Unchecked
W087_A001615	REAL32	Checked	Unchecked	Unchecked	Unchecked
W087_A001616	REAL32	Checked	Unchecked	Unchecked	Unchecked
W087_A001617	REAL32	Checked	Unchecked	Unchecked	Unchecked
W087_A001618	REAL32	Checked	Unchecked	Unchecked	Unchecked
W087_A001619	REAL32	Checked	Unchecked	Unchecked	Unchecked
W087_A001652	REAL32	Checked	Unchecked	Unchecked	Unchecked
W087_A001653	REAL32	Checked	Unchecked	Unchecked	Unchecked
W087_A001654	REAL32	Checked	Unchecked	Unchecked	Unchecked
W087_A001658	REAL32	Checked	Unchecked	Unchecked	Unchecked
W087_A001659	REAL32	Checked	Unchecked	Unchecked	Unchecked
W087_A001655	REAL32	Checked	Unchecked	Unchecked	Unchecked

DATA ITEM PERMISSIONS/NETWORK TYPE

For the data items added above (161 – 177):
  Check "W" (for write)
  Network Type = REAL32-Q (value: 20)

DATA SET (Definition)

Under "Remote: PEAK_RC":
Add Data Set Definition
  Name = PEAK_RC_IN
  IN/OUT = IN
  TRIGGER = PER
  Style = ALL
    Per = 10
    Grace = checked 90%

DATA SET (Contents)

Under "Content of: PEAK_RC_IN":
Add 17 Entries:
  DI/LS Index: 161 → 177

DATA ITEMS → Source

Set Data Items 161 → 177 to PEAK_RC (value: 4)

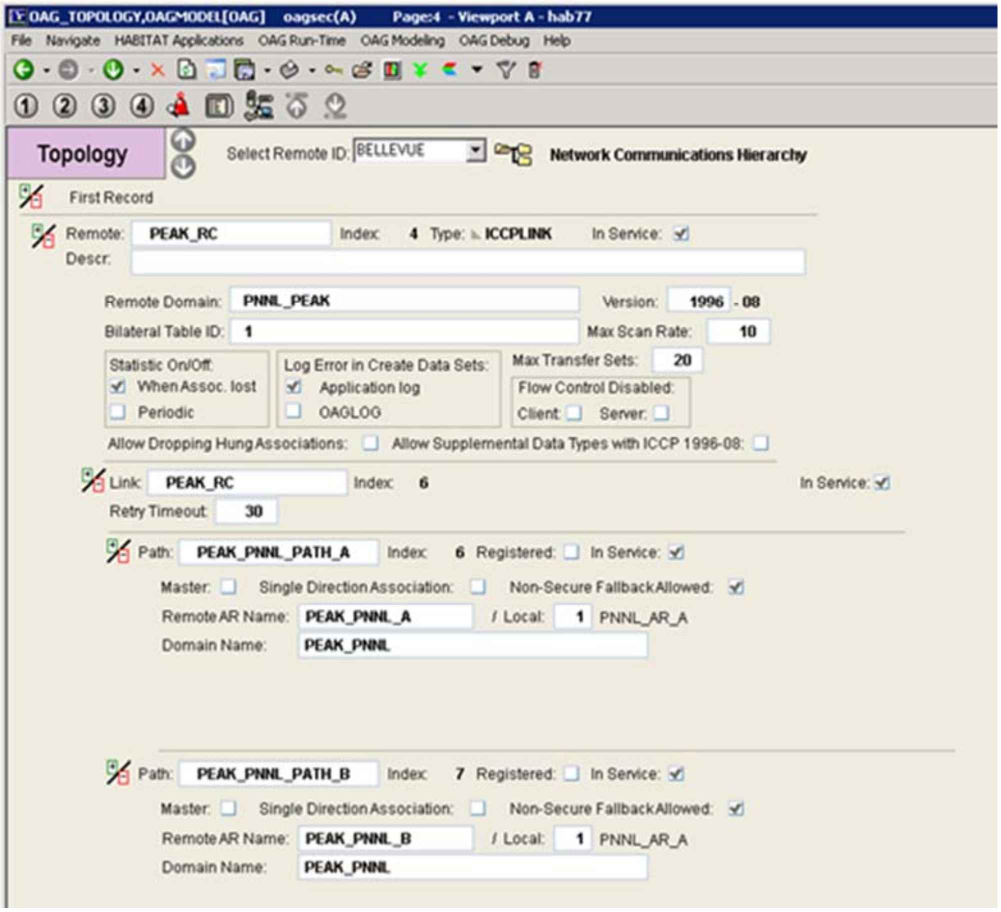
Validation and Deployment to Runtime

- Validate database – fix any errors
  - OAG Modeling → OAGMODEL Master
    - Push "Run Database Validation"
    - Check status on completion and fix errors
- Create Savecases of the OAGMODEL and OAGMOM
  - In the Top Text Box: YYYYMMDD
  - Habitat Applications → Savecase Manager → Savecase Manager Master
  - Click "OAGMODEL"
  - Click OAGMODEL → "Save"
  - Click OAGMOM → "Save"
- Stop all link applications and oagserve
  - Habitat Applications → Process Manager → Process Manager Master
  - Click "Stop" for all running link applications (ICCPLINK, ISDLINK, …)
  - Click "Stop" for OAGSERVE

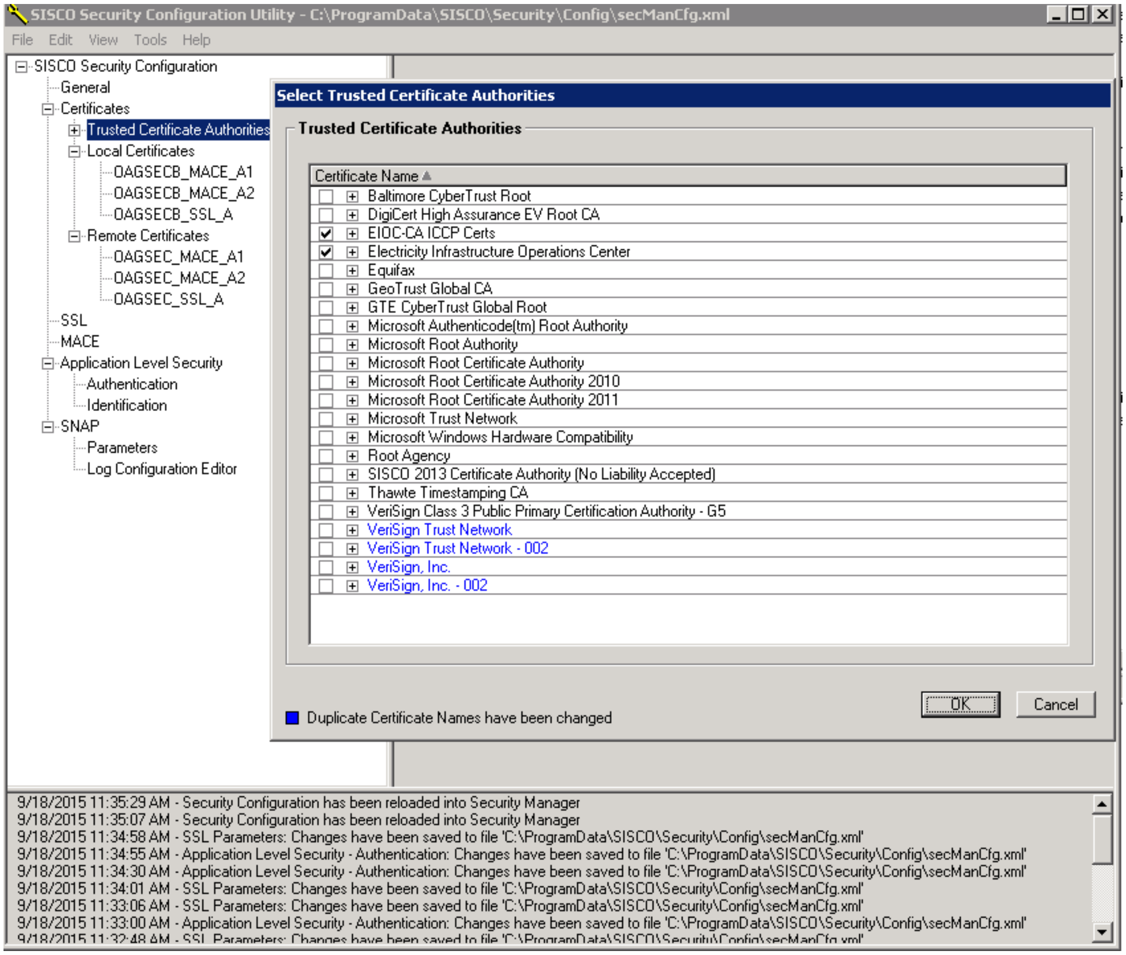
- Import model database to runtime environment
  - Verify that the textbox still has the YYYYMMDD in it
  - OAG Run-Time → OAGSERVE Master
  - Click the retrieve button (looks like a folder at the bottom of the page)
- Start oagserve and link applications
  - Habitat Applications → Process Manager → Process Manager Master
  - Click “Start” for OAGSERVE
  - Click “Start” for all running link applications (ICCPLINK, ISDLINK, …)
- Validate connection and data transfer
  - OAG Run-Time → Remote Directory
  - Click “PEAK_RC” button

Check

Screen captures of ICCP connection



- *Figure 5. PNNL OAG_A box configuration for the link with Peak RC*



- *Figure 6 SISCO Security Configurations*

Pacific Northwest
NATIONAL LABORATORY

U.S. DEPARTMENT OF
ENERGY

Proudly Operated by **Battelle** *Since 1965*

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99352
1-888-375-PNNL (7665)

www.pnnl.gov