Information Session on Alberta Reliability Standards Work Plan

August 10, 2021

AESO Engineering, Project Management & Technology

Using Zoom

- All attendees will join the meeting in listen-only mode, with attendee cameras disabled and microphones muted.
- When asking or typing in a question, **please state your first and last name and the organization you represent**.
- Two ways to ask questions during the presentation if you are accessing the meeting using your computer or smartphone:
  - You can **click the icon to raise your hand** and the host will see that you have raised your hand. The host will unmute your microphone. You in turn will need to unmute your microphone and then you can ask your question. Your name will appear on the screen, but your camera will remain turned off.
  - You can also ask questions by **typing them into the Q&A window**. Click the "Q&A" button next to "Raise Hand." You're able to up-vote questions that have been already asked.

Computer – where to access Zoom controls

- Using a 2-in-1/PC/Mac computer:
  - Hover your cursor over the bottom area of the Zoom window and the Controls will appear.
  - Click “Raise Hand” and the host will be notified that you would like to ask a question.
  - Click “Lower Hand” to lower it if needed.
  - You can also ask questions by tapping the “Q&A” button and typing them in. You’re able to up-vote questions that have been already asked.

Smartphone – where to access Zoom controls

- Using the Zoom app on a smartphone:
  - Tap “Raise Hand.” The host will be notified that you've raised your hand.
  - Tap “Lower Hand” to lower it if needed.
  - You can also ask questions by tapping the “Q&A” button and typing them in. You’re able to up-vote questions that have been already asked.

Phone-in – where to access Zoom controls

- If you are accessing the webinar via conference call:
  - If you would like to ask a question, on your phone's dial pad, hit ∗9 and the host will see that you have raised your hand. The host will unmute your microphone, you in turn will need to unmute your microphone by hitting ∗6 and then you can ask your question. Your number will appear on the screen.
- Phone controls for attendees:
  - To raise your hand, on your phone's dial pad, hit ∗9. The host will be notified that you've raised your hand.
  - To toggle between mute and unmute, on your phone's dial pad, hit ∗6.

AESO Stakeholder Engagement Framework

Stakeholder participation

- The participation of everyone here is critical to the engagement process. To ensure everyone has the opportunity to participate, we ask you to:
  - Listen to understand others' perspectives
  - Disagree respectfully
  - Balance airtime fairly
  - Keep an open mind

Welcome and Introductions

AESO meeting representatives

- Murray Mueller, Director, Operations Systems
- Ping-Kwan Keung, Manager, Standards & Modeling
- Ken Gardner, Reliability Standards Technical Advisor

Disclaimer

The information contained in this presentation is for information purposes only. While the AESO strives to make the information contained in this presentation as timely and accurate as possible, the AESO makes no claims, promises, or guarantees about the accuracy, completeness, or adequacy of the information contained in this presentation, and expressly disclaims liability for errors or omissions. As such, any reliance placed on the information contained herein is at the reader's sole risk.

Purpose of this session

- Provide information on status update on Alberta Reliability Standard Work Plan
- Background and development plan for CIP-012 Communications between Control Centers

Agenda

Item	Agenda Item
1	Introduction
2	Overview of August 2021 Alberta Reliability Standard program work plan
3	Questions and feedback from stakeholders
4	AESO Development Plan for adoption of CIP-012-a Communications between Control Centers • Background • Purpose of CIP-012 • Affordable reliability AESO plan for CIP-012-1 Adoption
5	Questions and discussion

Registrants (as of August 5, 2021)

- AltaLink Management Ltd.
- Alberta Newsprint Company
- ATCO Electric Ltd.
- Best Consulting Solutions Inc.
- Brookfield Renewable
- Capital Power Corporation
- City of Lethbridge
- City of Medicine Hat
- City of Red Deer
- CNRL
- Customized Energy Solutions
- DePal Consulting
- Enel Green Power
- ENMAX Power Corporation
- EPCOR Distribution & Transmission
- EPCOR Utilities
- GridSME
- Heartland Generation
- Market Surveilance Administrator
- Netsco
- NaturEner
- Northstone Power Corp.
- NRGCS
- Renewable Energy Systems
- Suncor Energy Inc.
- TransAlta Corporation

Overview of ARS Work Plan

- Walk-through of the August ARS work plan posted at:

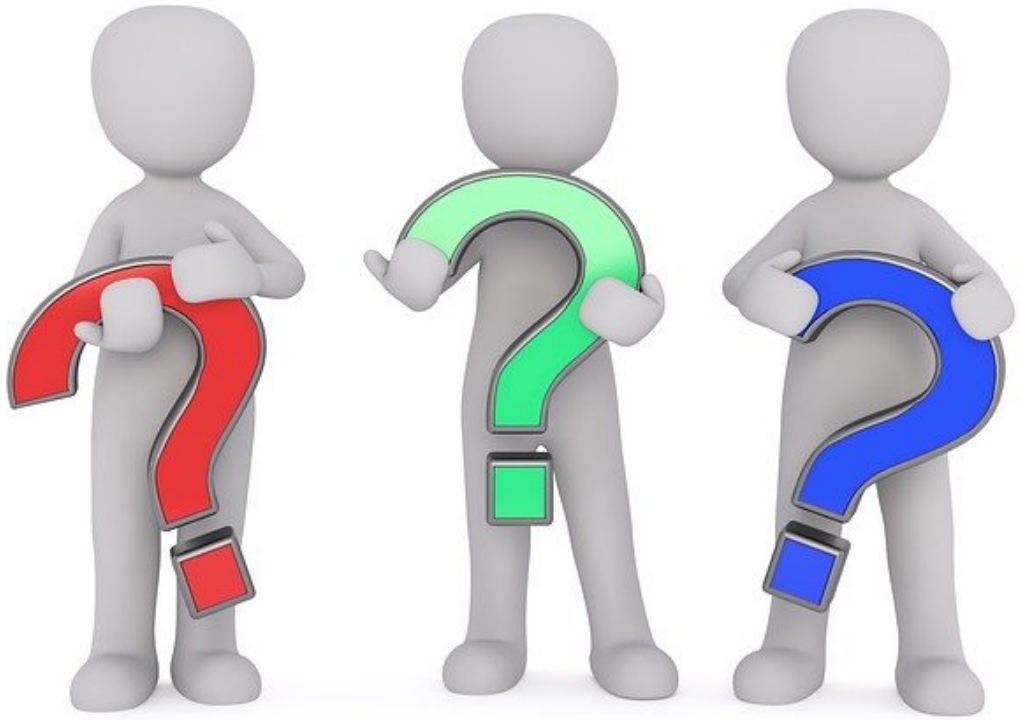
www.aeso.ca ►Rules, Standards and Tariff ►Alberta reliability standards ►Alberta reliability standards program work plan

- *https://www.aeso.ca/rules-standards-and-tariff/alberta-reliability-standards/*

Stakeholder feedback

- Request to circulate draft ARS prior to the information session.
- Request AESO External Compliance Monitoring Team to attend this session.
- Request to provide effective dates of these standards.

Questions



Cyber Security: Communications between Control Centers (CIP-012 Adoption)

Executive Summary

The AESO has implemented a modified version 5 of the NERC CIP cybersecurity standards within the set of Alberta Reliability Standards

CIP-012-1 – Cyber Security – Communications between Control Centers is a NERC standard to protect the *confidentiality and integrity of real-time assessment and real-time monitoring data transmitted* between control centers.

It requires the identification of security protection used, where it is applied, and where control centers are owned or operated by different responsible entities, the roles and responsibilities of each entity for applying security protection.

CIP-012 was recently approved by FERC as a new reliability standard that all US entities must be compliant with by *July 1st, 2022.*

Given the cyber risk and opportunity to implement CIP 012-1, AESO would like to align with the NERC July 1 2022 effective date

Potential Impacts to the **Bulk Electric System (BES)**

- Reliability
  - Automatic action based upon compromised application or data applicability questions
- Significant outages to the visibility of the Grid and Market
  - Restoration time - minutes to weeks
  - High cost to restore to normal
- Exposure of the BES to a higher threat vector
- Forced outages to actual BES assets
  - Generators, transformers, breakers and wind farms
- Market manipulation
  - Injection of false values to deliberately manipulate market

Background

- The AESO exchanges real-time monitoring and real-time assessment data with both internal and external entities to Alberta, to meet its mandate
- Different wide area networks (WANs) are used to transmit the data using different service providers; it is important to distinguish the external and internal work effort to integrate CIP-012-1 as they involve a different set of stakeholders

Cyber Risk Increasing

- Growing threats in cyber “space”
  - Many components that are vital to the BES, are connected through growing more complex networks, widening the attack surface for bad actors looking to infiltrate our critical infrastructure
  - With innovation comes new types of risks and new entry points for malicious actors to take advantage.
  - One of our primary concerns is over cyber attacks conducted remotely by hacking groups armed with malware, botnets, and stolen access credentials, including when data is in *transit*
- Adoption of CIP-012-1
  - CIP-012-1 presents several risk management, security, and compliance challenges

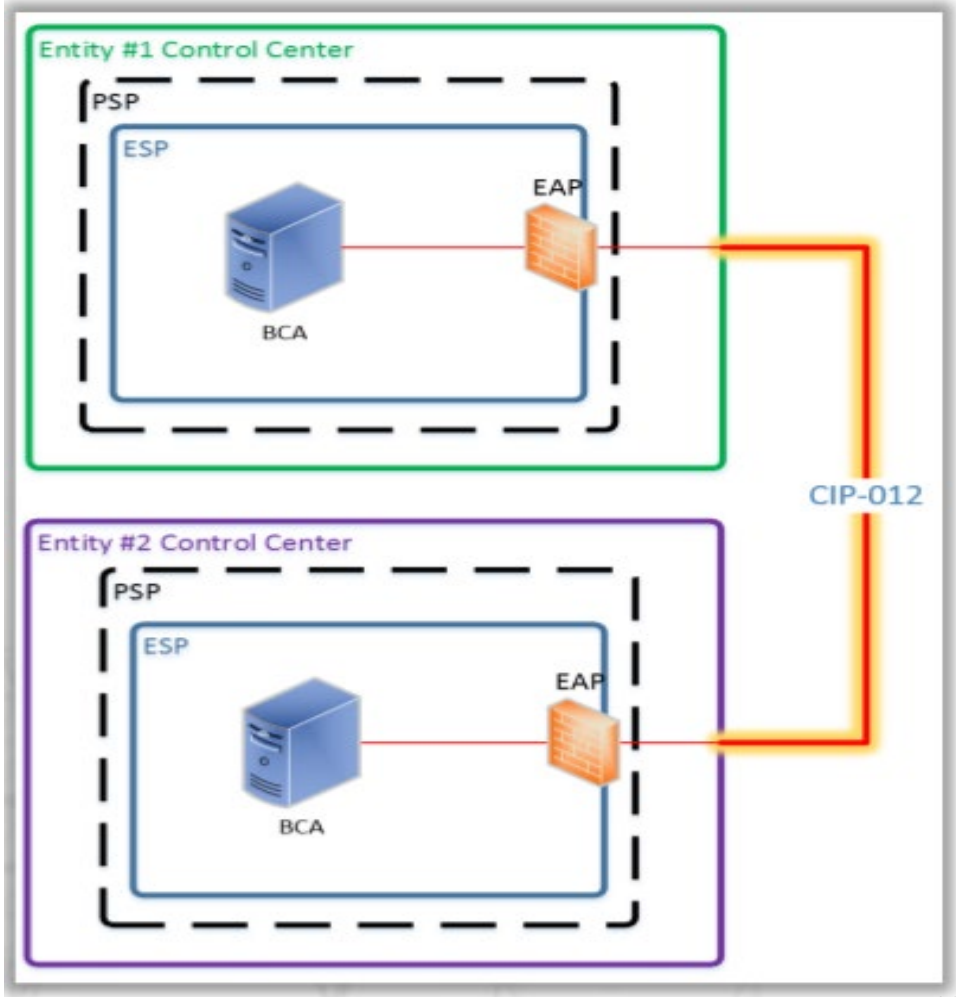
Purpose (CIP 012): Protection of Control Center Communications

Purpose: Protection of Real-time data transmitted between Control Centers

R1: Implement a plan to mitigate the risks of unauthorized disclosure or modification of ***data in transit:***

- Part 1.1: Identify the protection used
- Part 1.2: Identify where the protection was applied
- Part 1.3: Identify responsibilities of each entity when protection is shared

- Protection may be accomplished by:
  - Physically protecting the communication links
  - Logically protecting the data during transmission



Impacts: External to Alberta

- The AESO has been engaged by CAISO and other RC West members to implement protection on the ECN (Energy Communications Network), to satisfy CIP-012 compliance.
- The AESO will need to connect to a new, separate network for RC-RC data exchange.
- External data connections to WECC peers use the ECN (Energy Communications Network), sometimes also referred to as the WECC WON (WECC Operational Network). AT&T is the incumbent service provider and connects the AESO to other utility control centres at BC Hydro, CAISO, SPP, NERC, NorthWest Energy (NWE) and BPA.

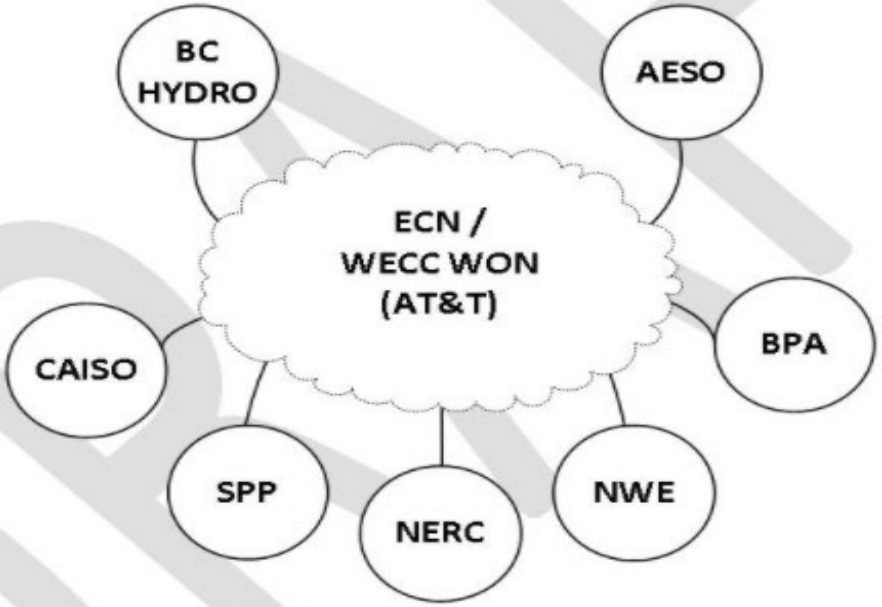


Figure 1: External entities the AESO exchanges data with across the ECN / WECC WON

Impacts: Internal to Alberta

- CIP-012 also applies to the connection between entities' primary and backup control centers

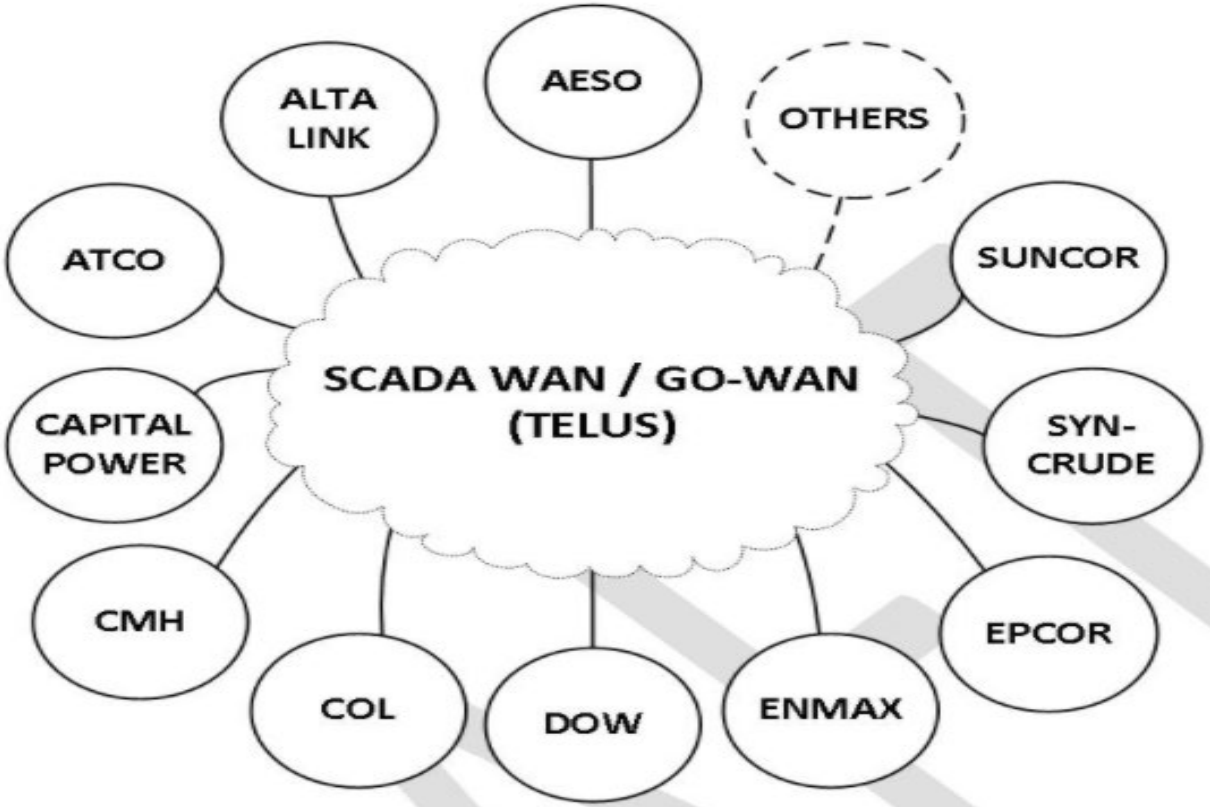
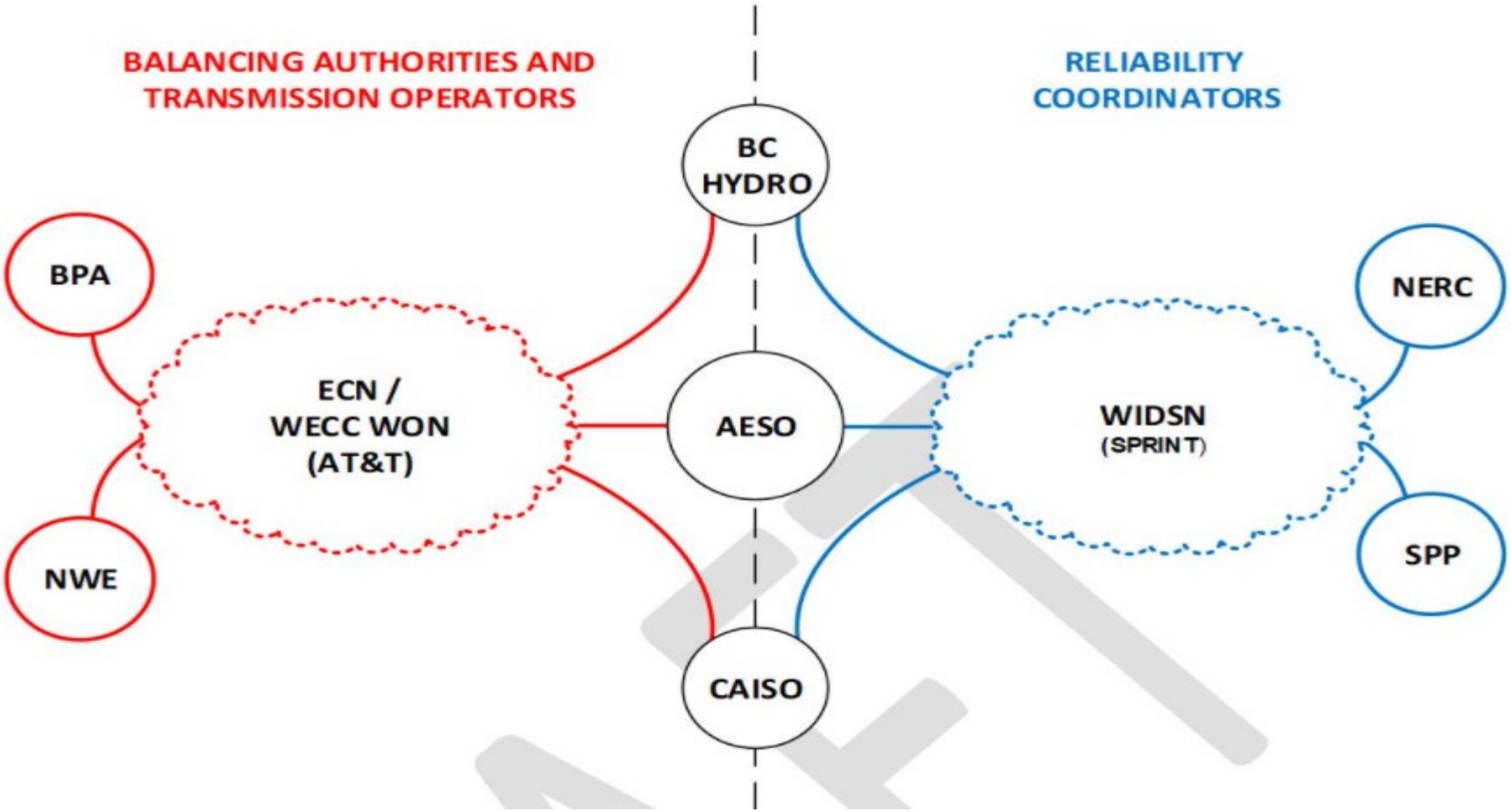


Figure 2: Internal entities the AESO exchanges data with across the SCADA WAN

Affordable Reliability for the BES

- Ensure the most cost-effective to way to secure our Networks

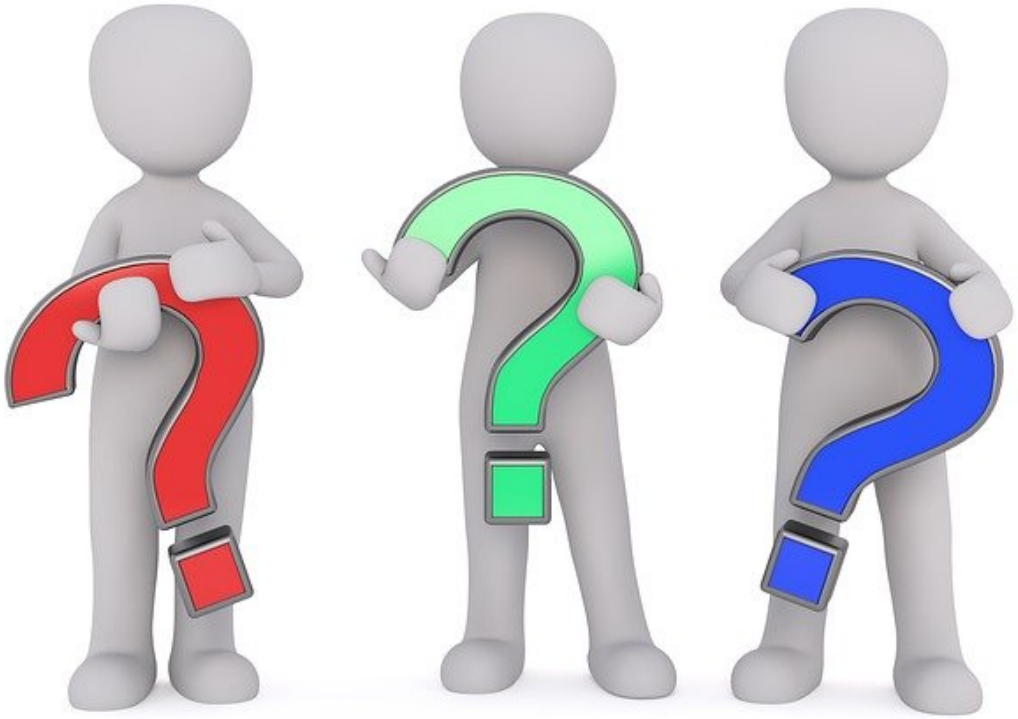


Alberta's plan for CIP 012-1 Adoption

1. Draft Standard – Q4 2021
   - Entities should review Cyber Security - Communications between Control Centers Technical Rationale and Justification for Reliability Standard CIP-012-1 prior to stakeholder consultation.

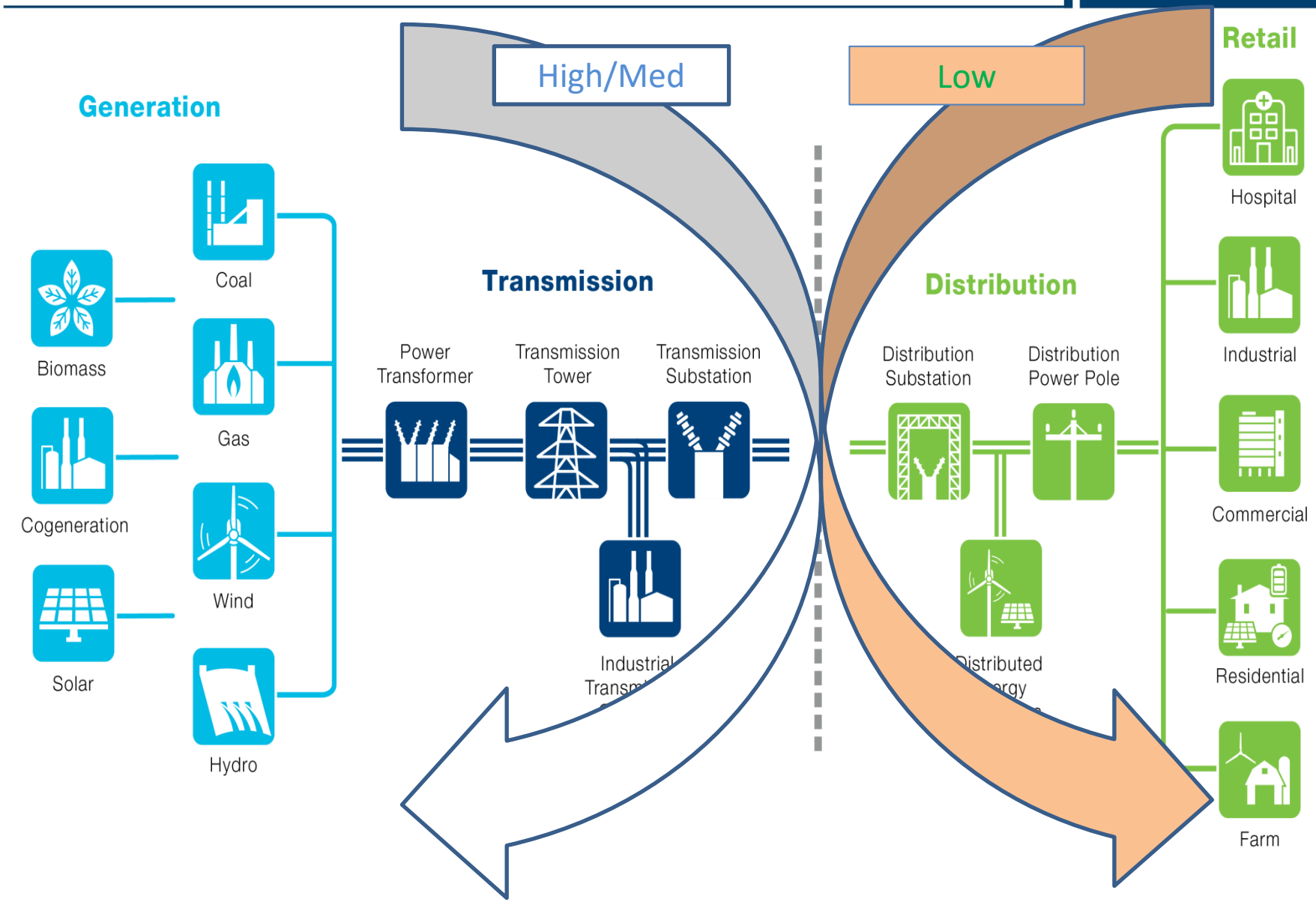
   a) Potential staged implementation/effective date (Proposed effective date for the ISO is July 1, 2022. Proposed effective date for other Alberta Entities is 4 full calendar quarters after approval by the Commission.)
2. Stakeholder Consultation – Q4 2021
   a) Post for stakeholder comments
   b) AESO reviews comments
   c) AESO responds to comments
3. Finalize and forward to Commission – Q4 2021

Questions and discussion



Appendix - Background Material

Applicability vs Risk



Technical Scope

- From NERC Cyber Security – Communications between Control Centers Technical Rationale and Justification for Reliability Standard CIP-012-1

As an example, Figure 5 shows several data transmissions between Control Centers that a Responsible Entity should consider to be in-scope. The example does not include all possible scenarios. The solid green lines are in-scope communications and the dashed red lines are out-of-scope communications.

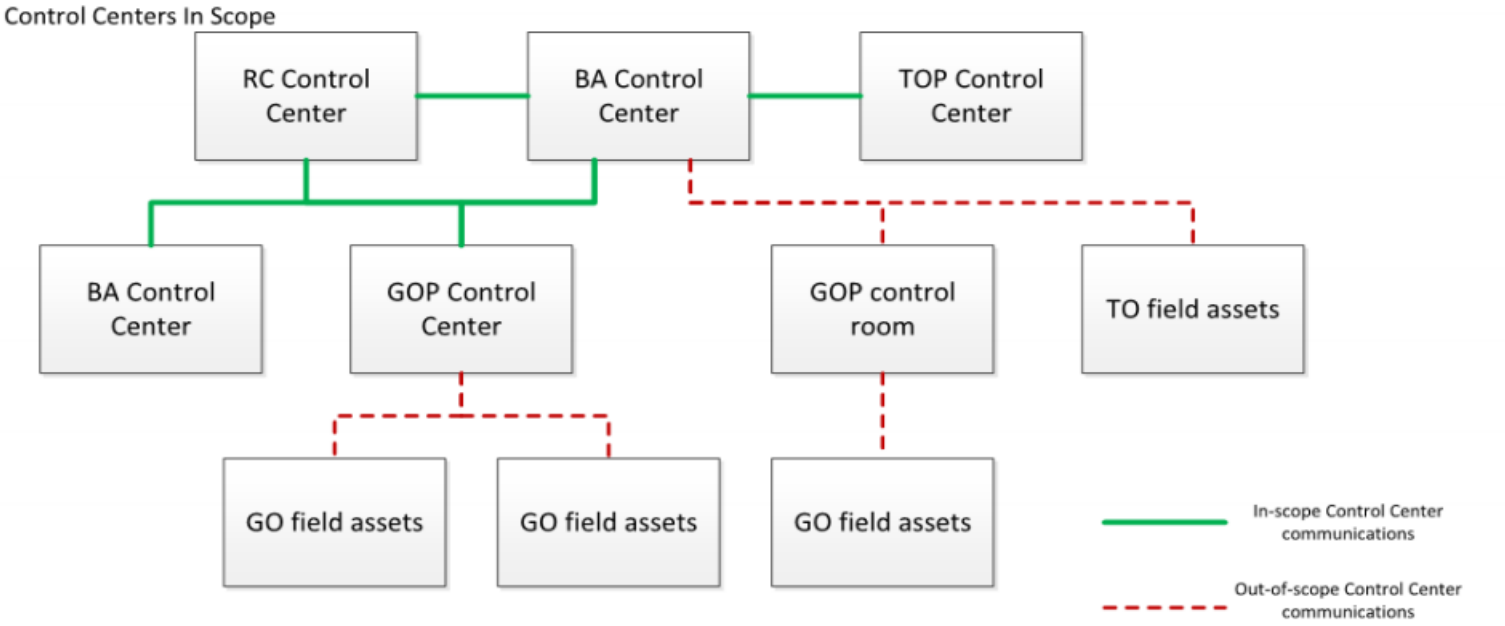


Figure 5: This reference model is an example and does not include all possible scenarios.

ICCP Servers are Typically BCS

- Historically (CIP V5), systems that provide “real-time inter utility data exchange” were viewed as Critical Cyber Assets
- For TFOs, ICCP can be a source of data used in performing Real Time Assessments
- For Gens, ICCP can be used in sending setpoints to power plants, fulfilling directives of the Balancing Authority
- An example where ICCP would not be considered BCS would be when exchanging data with a non-BES system, such as a Distribution System

Contact the AESO

- ***Twitter:*** *@theAESO*
- ***Website:*** *www.aeso.ca*
- Subscribe to our stakeholder newsletter

Thank you