WECC Reliability Coordination: Security Baseline and Configuration Management

Presented by **Lyonell D. Keplar**

Sr. Systems Administrator

Agenda

- Introduction
- WECC RC PI System Architecture
- Configuration Management
- Developing Security Baselines
- Questions

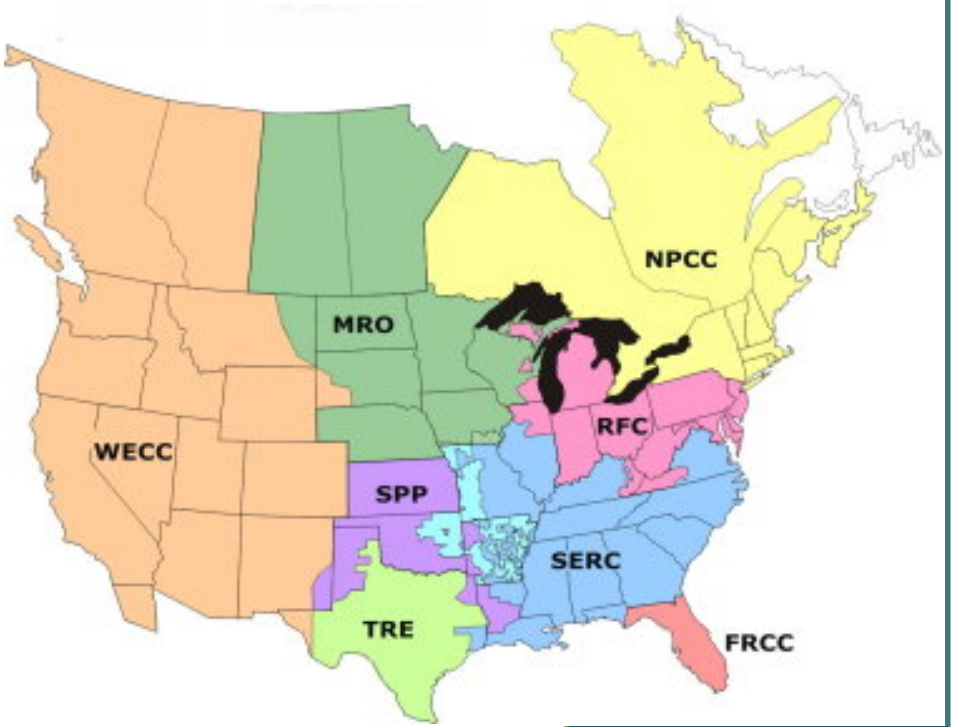
Introduction

Western Electricity Coordinating Council

- Formed in Response to the Northeast Blackout of 1965
  - 30 Million People and 80,000 Sq. Miles Impacted for 12 Hours
- Founded in 1967 as Western Systems Coordinating Council
  - Merged with two other regional associations in 2002 as WECC
- Headquartered in Salt Lake City, UT
- Exists to assure a reliable bulk electric system in the Western Interconnection

Introduction

- Largest Regional Entity Recognized by NERC and FERC
  - 1.8 Million Sq. Miles throughout North America
  - 126,285 Miles of Transmission Lines
  - 78 Million People



WECC

Introduction

- WECC Reliability Coordination
  - Offices in Vancouver, WA and Loveland, CO
- Provides Situational Awareness and Real-Time Supervision of the Western Interconnection
  - 24x7, 365 days a year
  - Large-scale telemetry data system feeds grid management tools, including the WECC RC PI System
  - Resulting models and tools are used by real-time RC staff to detect events within the Western Interconnection

© WECC 2012

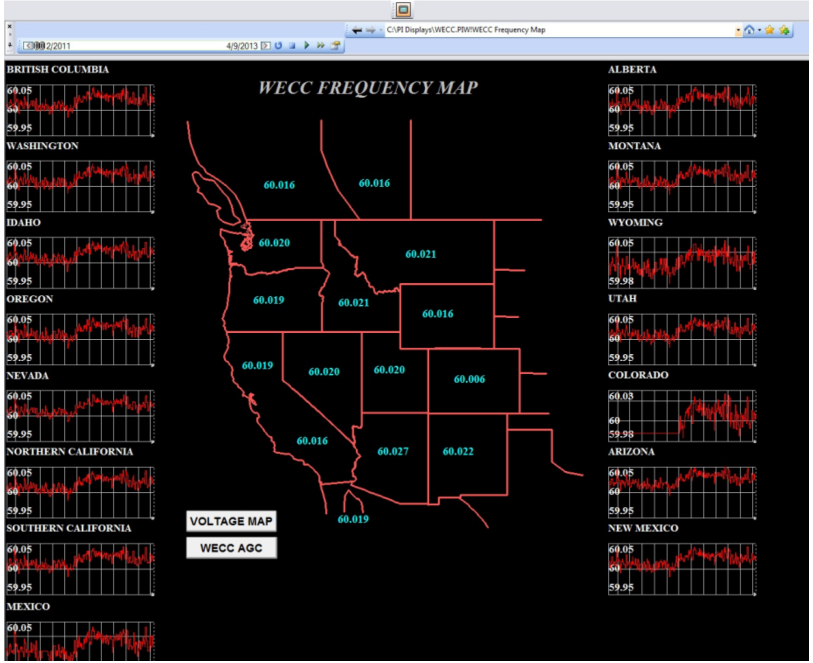
WECC

Introduction

- WECC RC – A Leader in SmartGrid Technology
  - Leading the Western Interconnection Synchrophasor Project
  - $107.8 million Smart Grid project, funded in part by the Department of Energy under the Smart Grid Investment Grant Program
  - 19 WISP participating entities (including WECC) are installing more than 400 new or upgraded Phasor Measurement Units (PMU) throughout the Western Interconnection
    - PMUs measures magnitude and phase angle of electricity
    - Real-time identification of system vulnerabilities and evolving disturbances
    - “Early Warning” system to help avoid widespread system blackouts

WECC RC PI System Architecture

- 72 PI Servers in Test and Prod
  - 10 PI ACE Servers
  - 10 PI Asset Framework Servers
  - 32 PI Interface Servers
  - 20 PI Servers
  - 1.7PB of Raw Storage



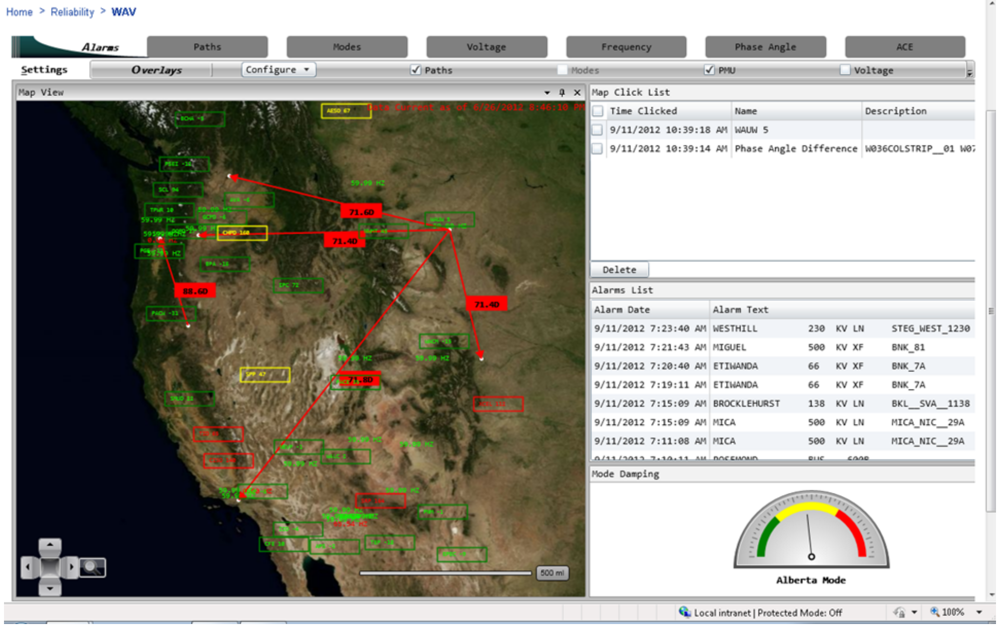
- 100% Uptime Requirement
  - Four-way redundancy
  - Test environment built identical to production

WECC RC PI System Architecture

- PI Server Collectives
  - ICCP Telemetry and EMS State Estimator
    - One production collective
    - 549,070 total measurements stored every 10 seconds
    - 1TB storage per year
  - Synchrophasor Telemetry
    - Two production collectives
    - Current Status: 2,000 measurements stored 30/second
    - Goal: 21,600 measurements stored 60/second
    - 60TB storage per year
- Total Telemetry Data
  - Current: 10,968,662,304,000 measurements/year
  - Goal: 85,141,334,304,000 measurements/year

WECC RC PI System Architecture

- WECC RC Internet Tools – Built on PI System
  - Common Situation Awareness Tools
  - Available to the Western Interconnection



Home > Reliability > **WAV**

Map Click List

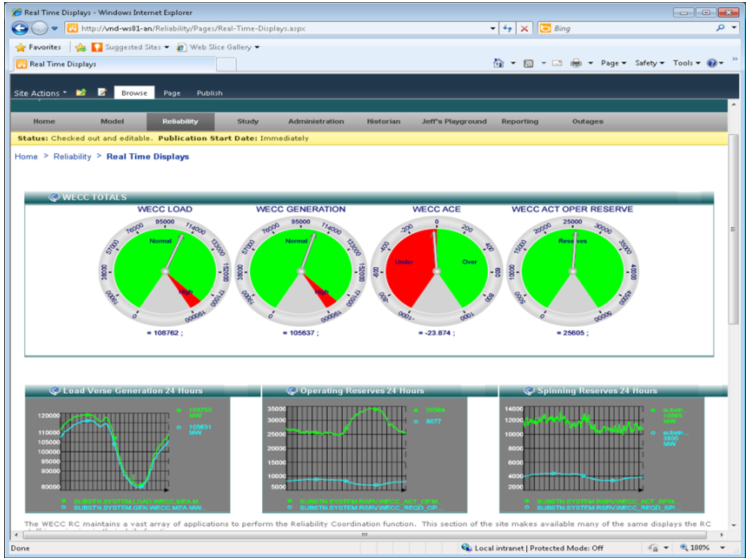
□	Time Clicked	Name	Description
□	9/11/2012 10:39:18 AM	WAUW 5	
□	9/11/2012 10:39:14 AM	Phase Angle Difference	W036COLSTRIP__01 W07

Alarms List

```
Alarm Date               Alarm Text
9/11/2012 7:23:40 AM     WESTHILL        230   KV LN    STEG_WEST_1230
9/11/2012 7:21:43 AM     MIGUEL          500   KV XF    BNK_81
9/11/2012 7:20:40 AM     ETIWANDA        66    KV XF    BNK_7A
9/11/2012 7:19:11 AM     ETIWANDA        66    KV XF    BNK_7A
9/11/2012 7:15:09 AM     BROCKLEHURST    138   KV LN    BKL__SVA__1138
9/11/2012 7:15:09 AM     MICA            500   KV LN    MICA_NIC__29A
9/11/2012 7:11:08 AM     MICA            500   KV LN    MICA_NIC__29A
9/11/2012 7:10:11 AM     ROSEMOND        BUS      6008
```

Mode Damping

Local intranet | Protected Mode: Off   100%



Real Time Displays - Windows Internet Explorer

http://vnd-ws01-an/Reliability/Pages/Real-Time-Displays.aspx

Status: Checked out and editable. **Publication Start Date:** Immediately

Home > Reliability > **Real Time Displays**

WECC TOTALS

= 108762 ; = 105637 ; = -23.874 ; = 25605 ;

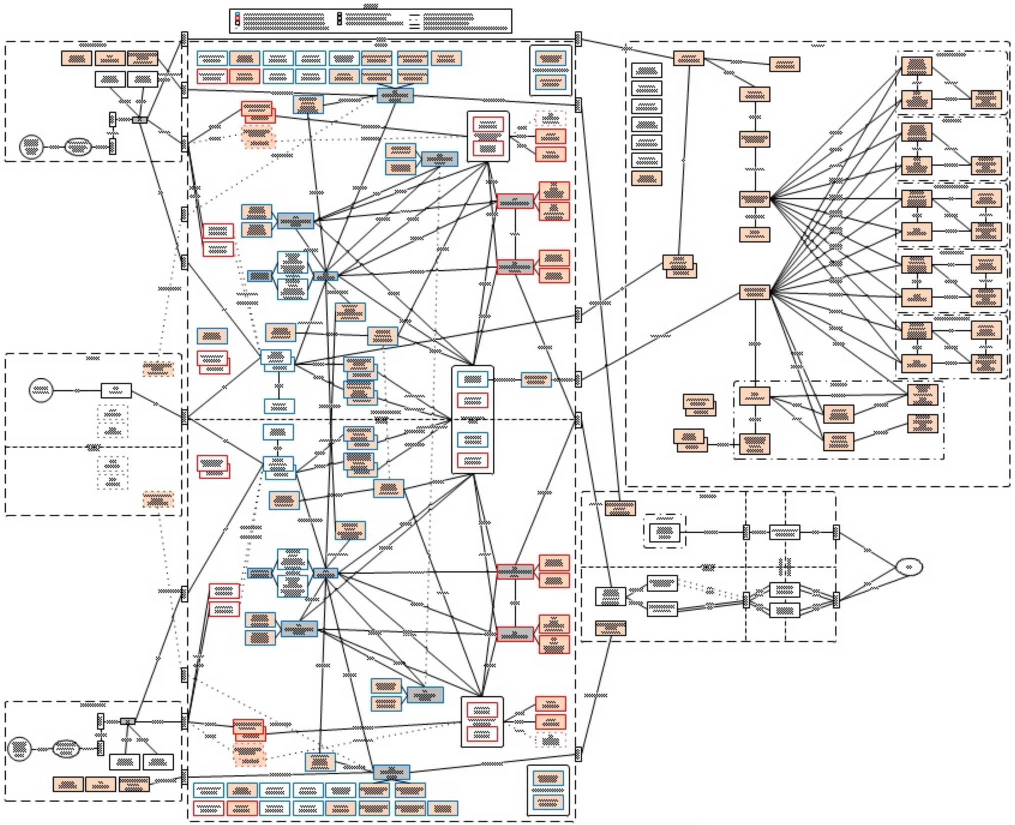
Load Verse Generation 24 Hours
120000
110000
105000
100000
95000
90000
80000
108755 MW
105631 MW
SUBSTN.SYSTEM.LOAD.WECC.MEA.M...
SUBSTN.SYSTEM.GEN.WECC.MEA.MW...
Operating Reserves 24 Hours
35000
30000
25000
20000
15000
10000
5000
25564
8077
SUBSTN.SYSTEM.RSRV.WECC_ACT_OP.M...
SUBSTN.SYSTEM.RSRV.WECC_REQD_OP...
Spinning Reserves 24 Hours
14000
12000
10000
8000
6000
4000
2000
substn... 10665 MW
substn... 3806 MW
SUBSTN.SYSTEM.RSRV.WECC_ACT_SPIN...
SUBSTN.SYSTEM.RSRV.WECC_REQD_SPI...

The WECC RC maintains a vast array of applications to perform the Reliability Coordination function. This section of the site makes available many of the same displays the RC

Done   Local intranet | Protected Mode: Off   100%

Configuration Management

- Why do we focus so strongly on configuration management?
  - Small team – 17 Staff
    - 8 Person IT Team
    - 9 Person App Support Team
  - Large, complex environment
  - Downtime is not an option!
  - I have no more hair to lose
- How Complex?
  - This is a logical diagram of our test environment



Configuration Management

- Consistent and Dynamic Change Management
  - Middleware used to track changes to systems automatically
  - Daily port scans and systems scans used to determine change status
  - Effective automation means changes can be approved rapidly, with confidence that the change will be tracked and managed appropriately

Configuration Management

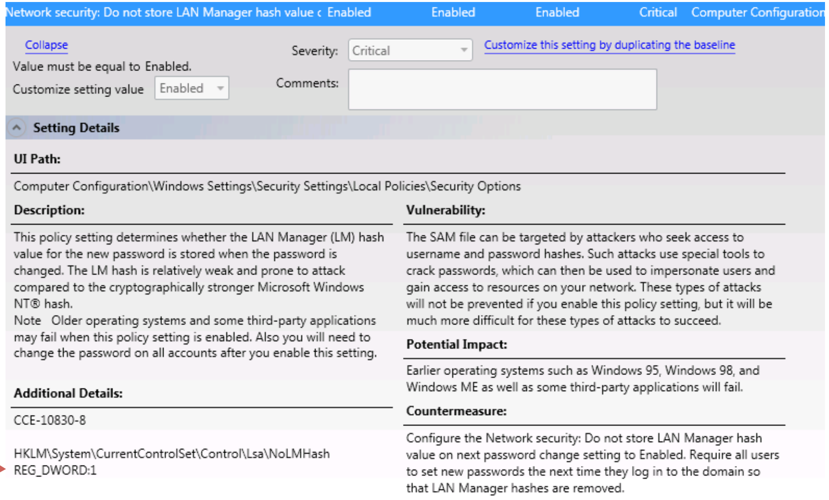
- Effective Change Management
  - A good change management process should facilitate implementing change – it shouldn’t hinder implementing change
  - You must have a baseline - how your systems SHOULD be configured
    - Security settings
    - ACLs and permissions on the system
    - Installed applications, firmware and driver revisions
    - Services available on the system
  - Analyze changes to determine when and what is deviated from your established baseline
    - Analysis of each of the components of your baseline
    - Look for automation in the process – manual review can unnecessarily hinder the process

Security Baselines

- Our Approach to Security Baselines
  - Don’t Reinvent the Wheel
    - Vendors provide tools and documentation
    - Example: Microsoft Security Compliance Manager Toolkit
    - Example: Cisco Network Security Baseline Documentation
  - Risk-Based Assessment
    - Evaluate the risk of each setting
    - Determine risk mitigation, if applicable
  - Document the Settings for Ongoing Assessment
    - Change management: Compare baseline settings before and after changes
    - Use of middleware tools can automate this process
    - Regulated and audited industry? Use vendor documentation as evidence for compliance!

Security Baselines

- Microsoft Security Compliance Manager
  - ○ Provides guidance on the security settings available in the Windows operating system
  - ○ Defines recommended policy settings for Windows operating system, both servers and workstations
  - ○ Provides the registry key that implements the setting →



Network security: Do not store LAN Manager hash value c Enabled Enabled Enabled Critical Computer Configuration

Severity: Critical

Value must be equal to Enabled.

Customize setting value Enabled

Comments:

UI Path:

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

Description:

This policy setting determines whether the LAN Manager (LM) hash value for the new password is stored when the password is changed. The LM hash is relatively weak and prone to attack compared to the cryptographically stronger Microsoft Windows NT® hash.
Note Older operating systems and some third-party applications may fail when this policy setting is enabled. Also you will need to change the password on all accounts after you enable this setting.

Additional Details:

CCE-10830-8

HKLM\System\CurrentControlSet\Control\Lsa\NoLMHash
REG_DWORD:1

Vulnerability:

The SAM file can be targeted by attackers who seek access to username and password hashes. Such attacks use special tools to crack passwords, which can then be used to impersonate users and gain access to resources on your network. These types of attacks will not be prevented if you enable this policy setting, but it will be much more difficult for these types of attacks to succeed.

Potential Impact:

Earlier operating systems such as Windows 95, Windows 98, and Windows ME as well as some third-party applications will fail.

Countermeasure:

Configure the Network security: Do not store LAN Manager hash value on next password change setting to Enabled. Require all users to set new passwords the next time they log in to the domain so that LAN Manager hashes are removed.

Security Baselines

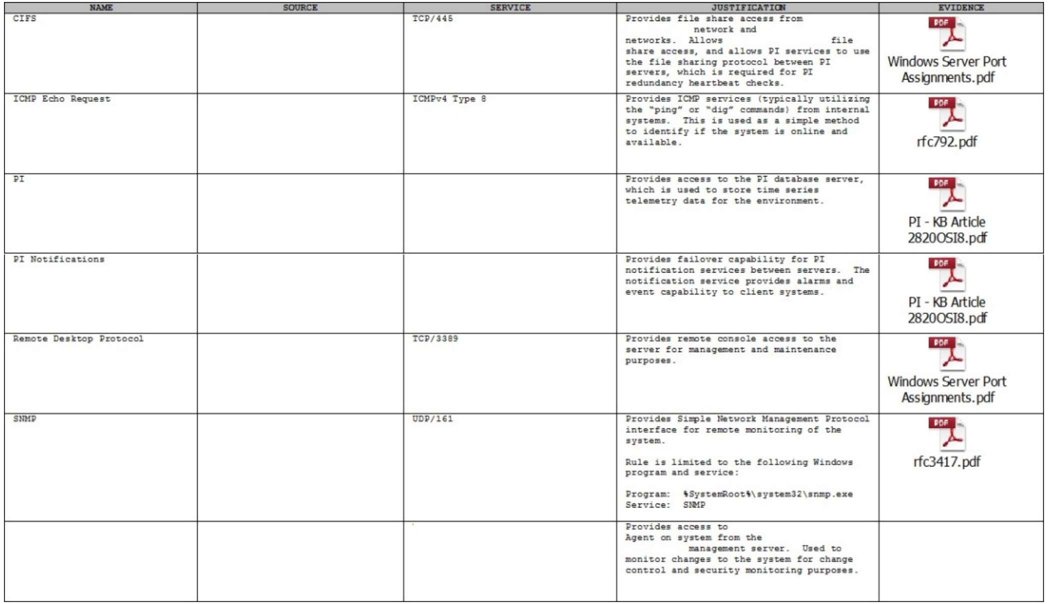
- Ports and Services
  - Limit the surface footprint of systems to the minimum required for the system to perform its job function
  - PI Database Servers have only one inbound port open to them from workstations (PI Network Manager)
  - Review and research vendor documentation to determine the minimum required

```
Starting Nmap 6.25 ( http://nmap.org )
Nmap scan report
Host is up (0.0010s latency).

PORT      STATE SERVICE
5450/tcp  open    unknown
```

Security Baselines

- Port Scanning – Available Services
  - Daily delta scans against established baselines
  - Tools that identify the service based on the response, not just the port and protocol



NAME	SOURCE	SERVICE	JUSTIFICATION	EVIDENCE
CIFS		TCP/445	Provides file share access from network and networks. Allows file share access, and allows PI services to use the file sharing protocol between PI servers, which is required for PI redundancy heartbeat checks.	PDF Windows Server Port Assignments.pdf
ICMP Echo Request		ICMPv4 Type 8	Provides ICMP services (typically utilizing the "ping" or "dig" commands) from internal systems. This is used as a simple method to identify if the system is online and available.	PDF rfc792.pdf
PI			Provides access to the PI database server, which is used to store time series telemetry data for the environment.	PDF PI - KB Article 2820OSI8.pdf
PI Notifications			Provides failover capability for PI notification services between servers. The notification service provides alarms and event capability to client systems.	PDF PI - KB Article 2820OSI8.pdf
Remote Desktop Protocol		TCP/3389	Provides remote console access to the server for management and maintenance purposes.	PDF Windows Server Port Assignments.pdf
SNMP		UDP/161	Provides Simple Network Management Protocol interface for remote monitoring of the system. Rule is limited to the following Windows program and service: Program: %SystemRoot%\system32\snmp.exe Service: SNMP	PDF rfc3417.pdf
			Provides access to Agent on system from the management server. Used to monitor changes to the system for change control and security monitoring purposes.	

Security Baselines

Baseline Policy

- Contains policy settings common to all systems
- WECC RC baseline defines 497 settings
  - Example: Removable media restriction
- Includes automated middleware application deployments

System Type Policy

- Contains policy settings that deviate from the common baseline
  - Example: Enabling 8.3 NTFS name creation
- Contains the host firewall rules for the system type
- System type application deployments

References

- Microsoft Security Compliance Manager

http://technet.microsoft.com/en-us/library/cc677002.aspx

- Cisco Network Security Baseline

http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/Baseline_Security/securbase.pdf

Questions?

Lyonell D. Keplar

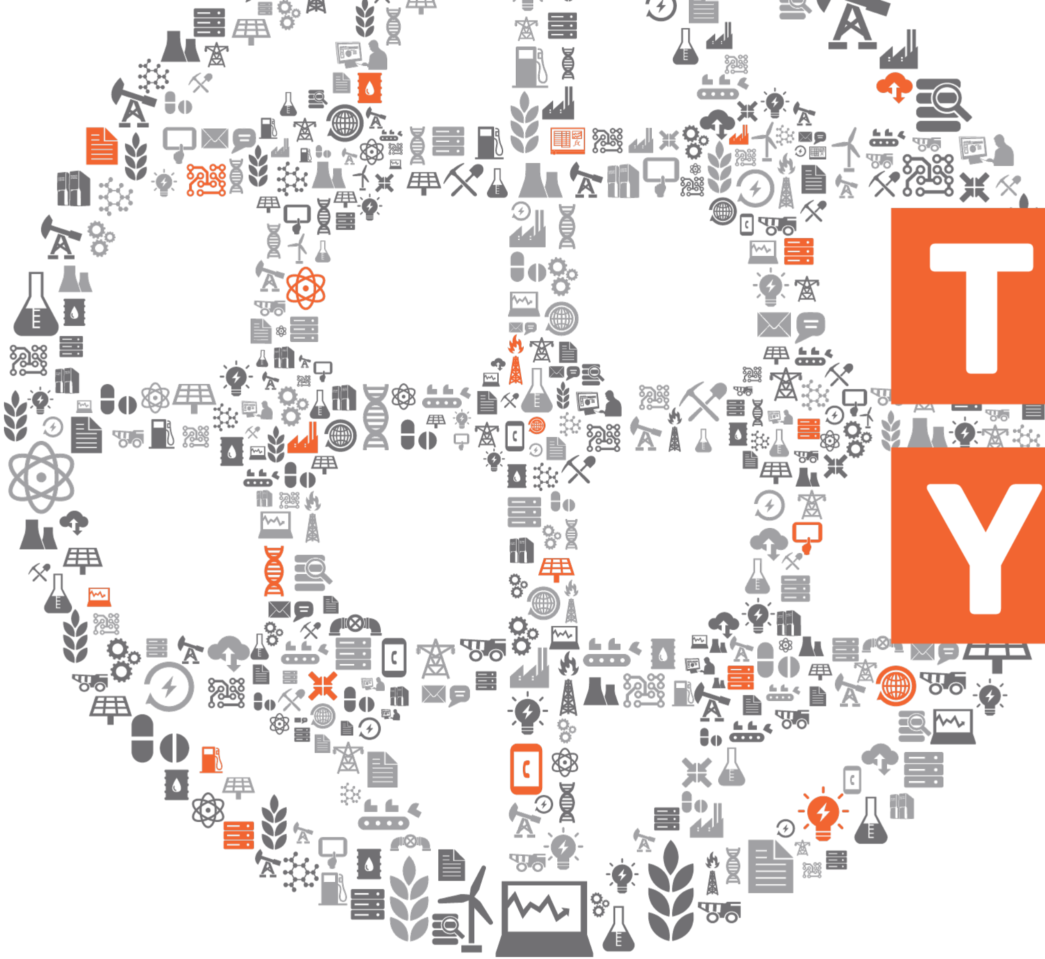
lkeplar@wecc.biz

Lyonell D. Keplar

lkeplar@wecc.biz

Sr. Systems Administrator

WECC



THANK YOU

Brought to you by

OSIsoft.