OSIsoft® UC 2010

Real Time Information — Currency of the New Decade

Hilton San Francisco Union Square | San Francisco, CA

April 26-28, 2010

Managing Security, Risk and Compliance for Critical Assets on the Smart Grid

Kshamit Dixit

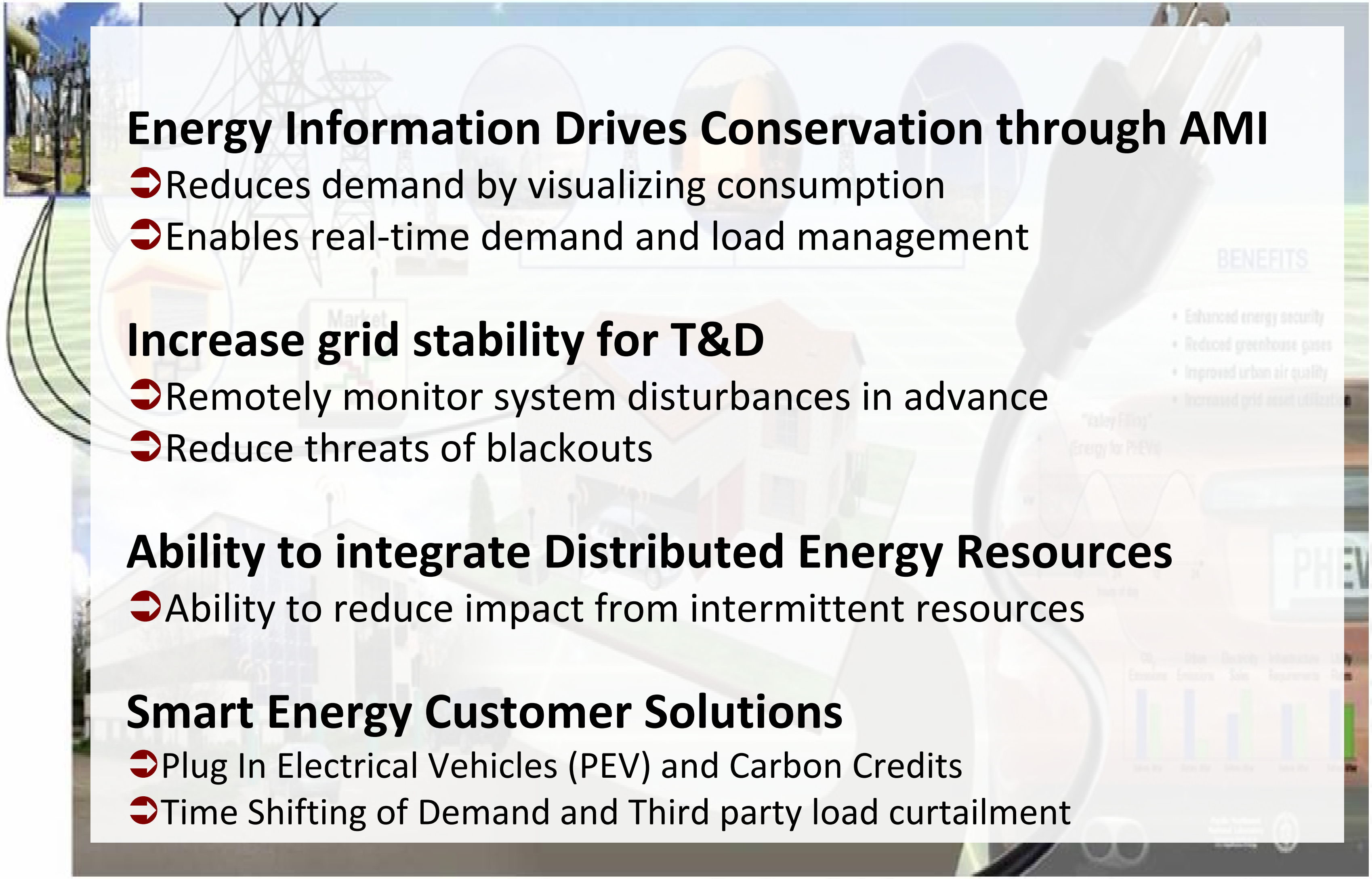
Toronto Hydro

Toronto Hydro– A snapshot

- **Worldwide Employees: 1,700**
- **Revenues: $2.3 Billion**
- **Headquarters: Toronto, Ontario**
- **Government Owned Vertically Integrated Electric Utility: Regulated and Unregulated operating holdings:**
- **<u>Toronto Hydro Corporation</u>**
  - ***Toronto Hydro Electric System Limited***
  - ***Toronto Hydro Energy Services Inc.***

toronto hydro

Smart Grid Can Deliver…



Energy Information Drives Conservation through AMI

- Reduces demand by visualizing consumption
- Enables real-time demand and load management

Increase grid stability for T&D

- Remotely monitor system disturbances in advance
- Reduce threats of blackouts

Ability to integrate Distributed Energy Resources

- Ability to reduce impact from intermittent resources

Smart Energy Customer Solutions

- Plug In Electrical Vehicles (PEV) and Carbon Credits
- Time Shifting of Demand and Third party load curtailment

Smart Grid Poses New Challenges

- Protecting privacy and privileged access to smart meters, gateways and aggregated meter data.
- Power/flexibility of smart meters brings additional security challenges (e.g. remote disconnect)
- Active involvement of Consumer
- Segregation Of Duties: billing, meter data access
- Additional regulations…

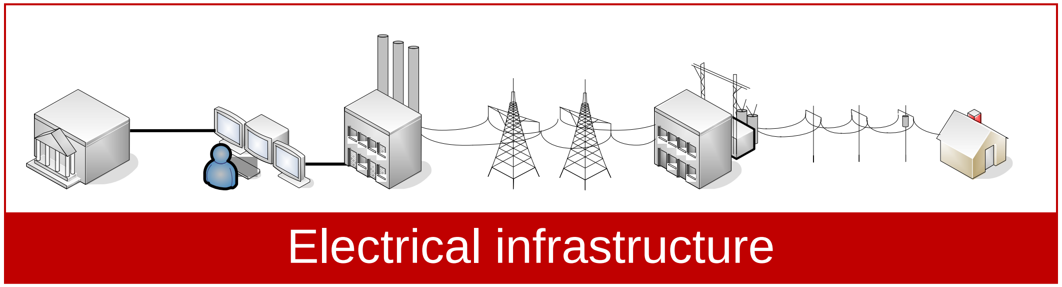
Traditional Threats, Risks, Security Challenges for Utilities

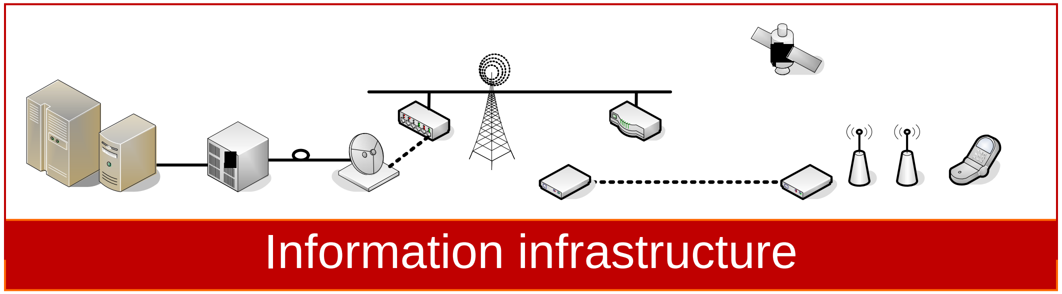
- Identifying and Securing Critical Assets
- Securing Physical Access to assets and facilities
- Securing SCADA and other real-time control applications
- Risk analysis across operational systems: On-boarding / Off-boarding and Background Checks
- Privileged User, “Access Creep”
- Insider threat - monitoring access & behavior
- Situational Awareness (Command & Control)

Utilities' Imperative for Security

- **Protection of Operating Assets and Reliability**
  - – Securing Cyber Critical Assets
  - – Securing Safety Systems for key Grid Components
  - – Ensuring continuity of operations and mitigating risks of revenue interruption
- **Regulatory Compliance**
  - – Cost and complexity of regulations is growing
  - – Imperative to implement a risk-based continuous compliance

Smart Grid is driving the integration of two infrastructures…

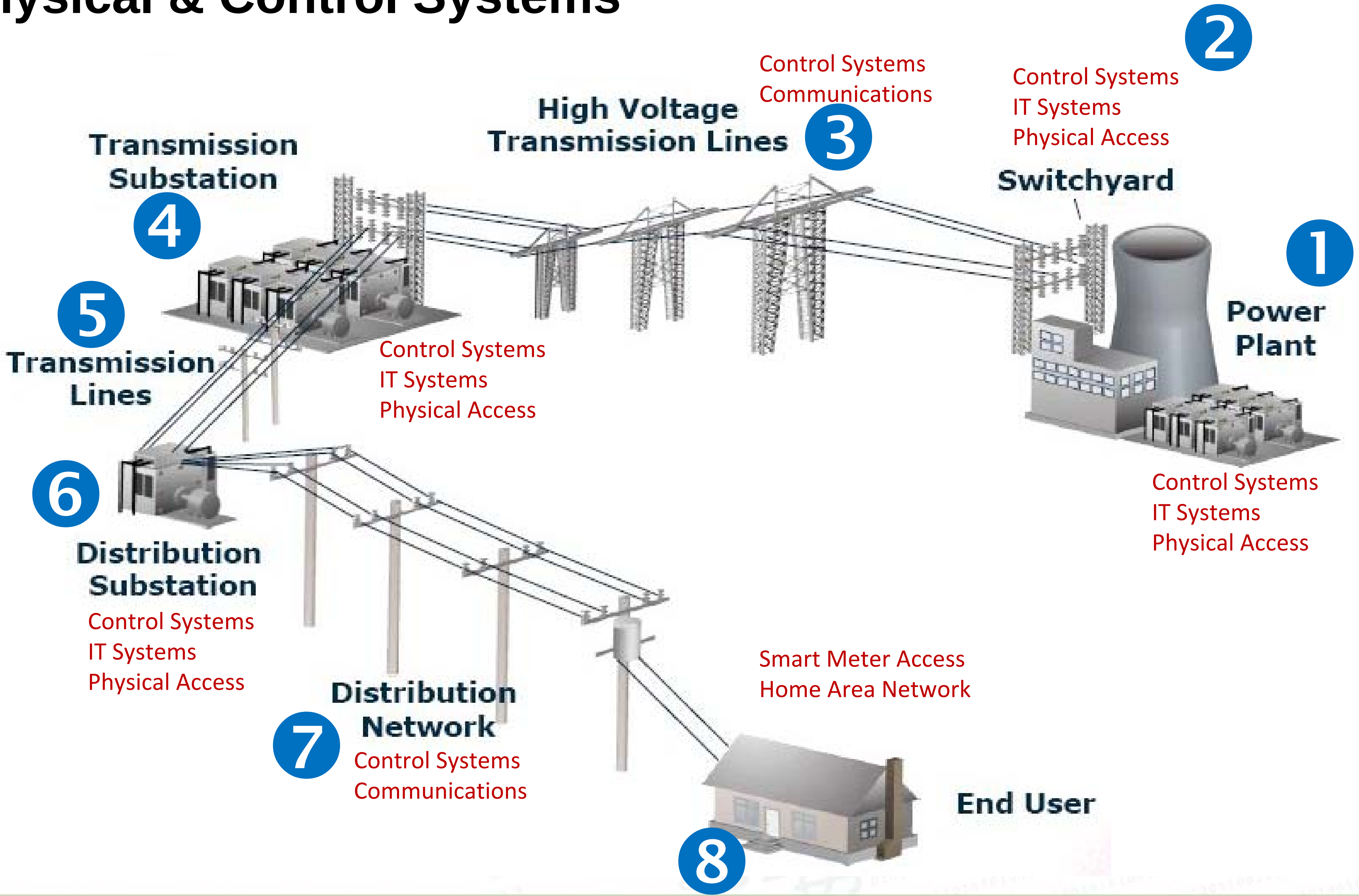

Electrical infrastructure


Information infrastructure

- Integration between plant operations and business
- Real-time monitoring for power quality and reliability
- Demand and consumption monitoring
- Integrating alternative energy sources

Securing these combined infrastructures requires a new approach to security that addresses blended threats through the convergence of IT Security, Physical Access Security and Control System Security.

Points To Secure Along the New Energy Supply Chain – IT, Physical & Control Systems



1 Power Plant

Control Systems
IT Systems
Physical Access

2 Switchyard

Control Systems
IT Systems
Physical Access

3 High Voltage Transmission Lines

Control Systems
Communications

4 Transmission Substation

Control Systems
IT Systems
Physical Access

5 Transmission Lines

6 Distribution Substation

Control Systems
IT Systems
Physical Access

7 Distribution Network

Control Systems
Communications

8 End User

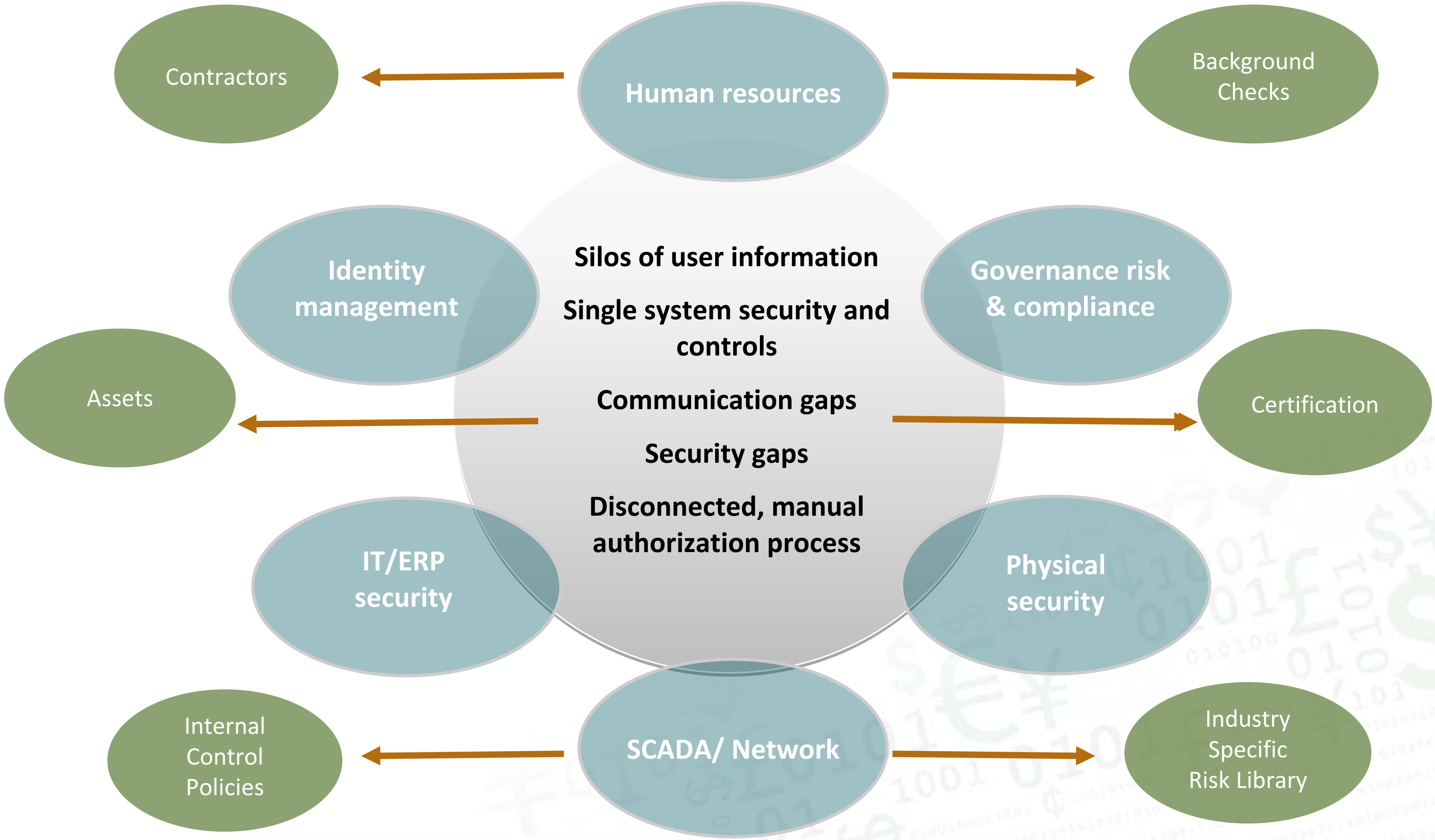
Smart Meter Access
Home Area Network

Security convergence is the only way to secure the entire energy chain..

Manage Security and Risk across IT, Physical Access and Control Systems

- Protecting privacy and privileged access to smart meters, gateways and aggregated meter data.
- Identifying and Securing Critical Assets
- Securing Physical Access to assets and facilities
- Securing SCADA and other real-time control applications
- Risk analysis across operational systems: On-boarding / Off-boarding and Background Checks

Too Many Silos of Information



Silos of user information

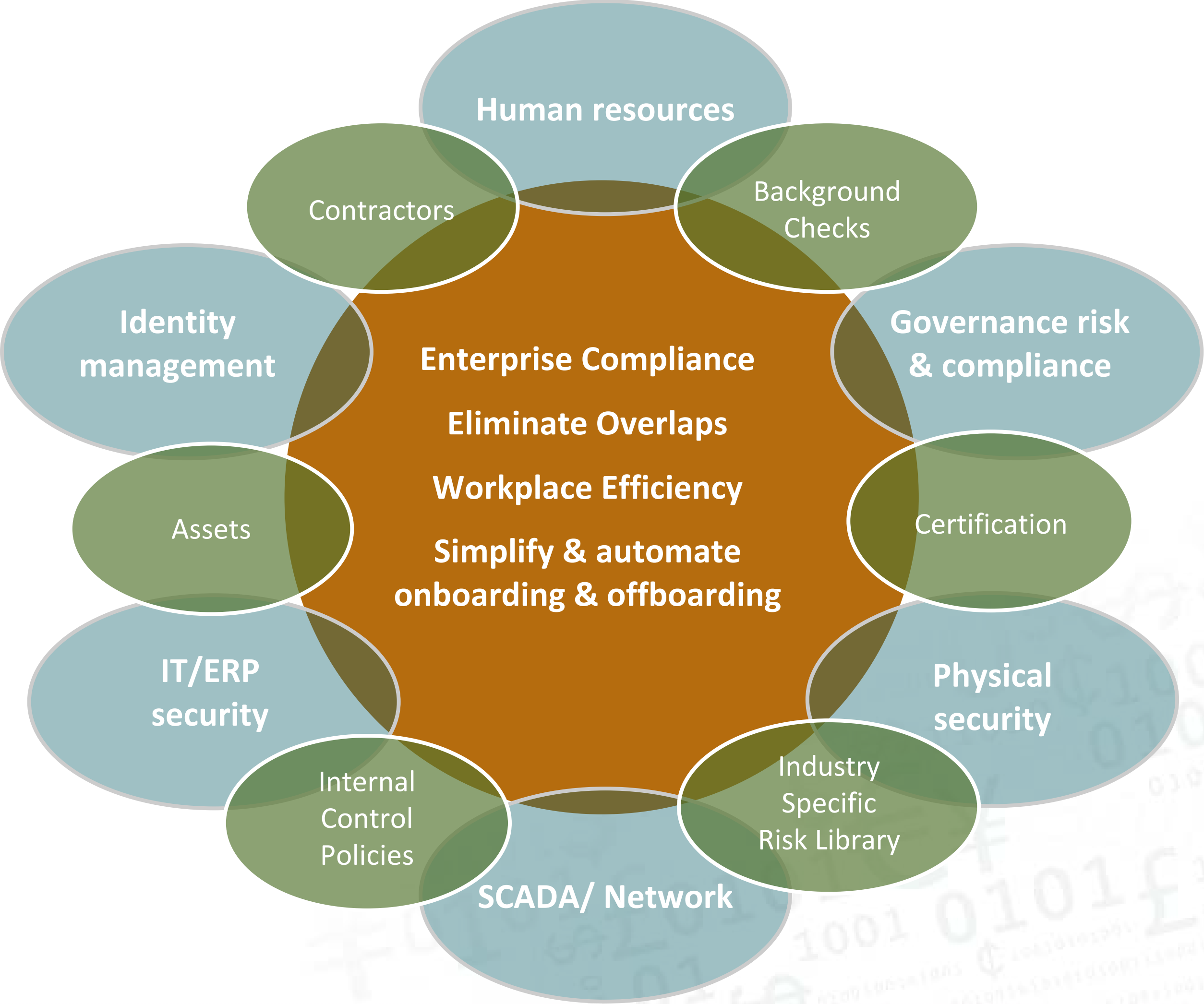
Single system security and controls

Communication gaps

Security gaps

Disconnected, manual authorization process

Unifying Application Needed to Close Security Gaps



Enterprise Compliance

Eliminate Overlaps

Workplace Efficiency

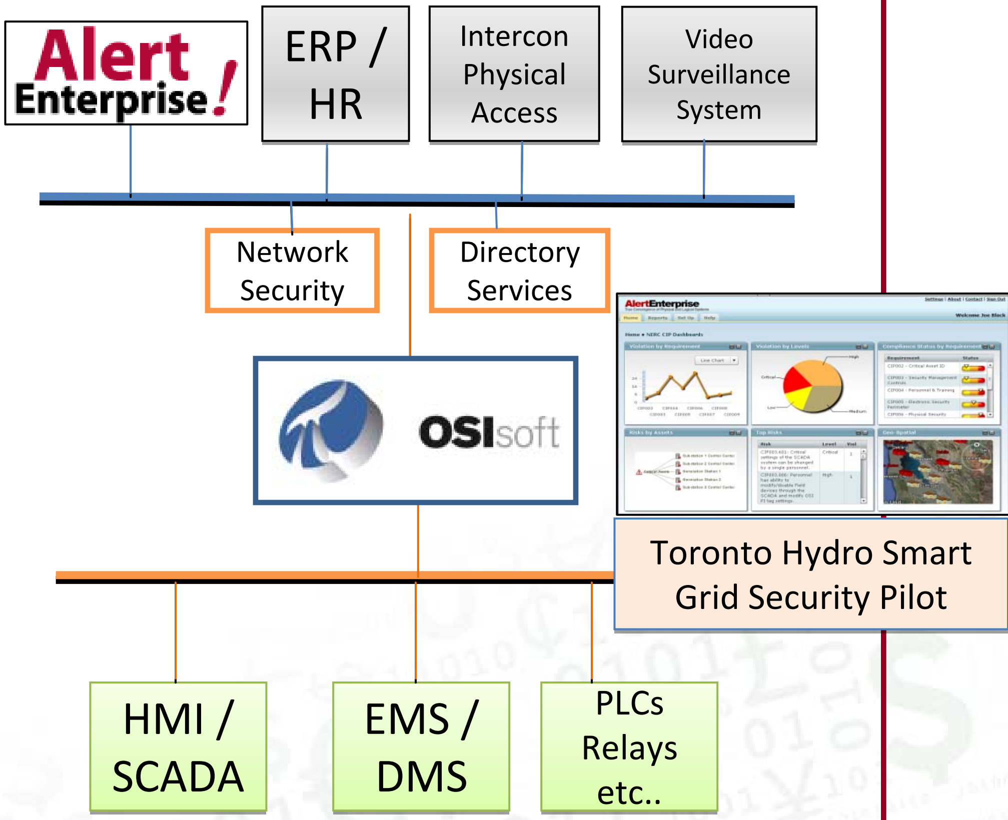
Simplify & automate onboarding & offboarding

Implementing a Risk-Based Approach to Security

- Identify critical assets – implement controls in order of criticality
- Adopt standards and frameworks to augment organization specific policies
- An integrated risk and compliance automation solution can combine standards, frameworks and policies in an integrated approach
- Adopt a solution that can extend beyond just Controls Documentation and automate controls testing for IT and Physical Access Controls by breaking down the silos.
- Aggregating risks and events from industrial control systems completes the risk picture for asset-intensive environments like the Smart Grid.
- Real-time access to information via roles-based dashboards and incident management screens with built-in guidance allows situation managers to address threats as they unfold.

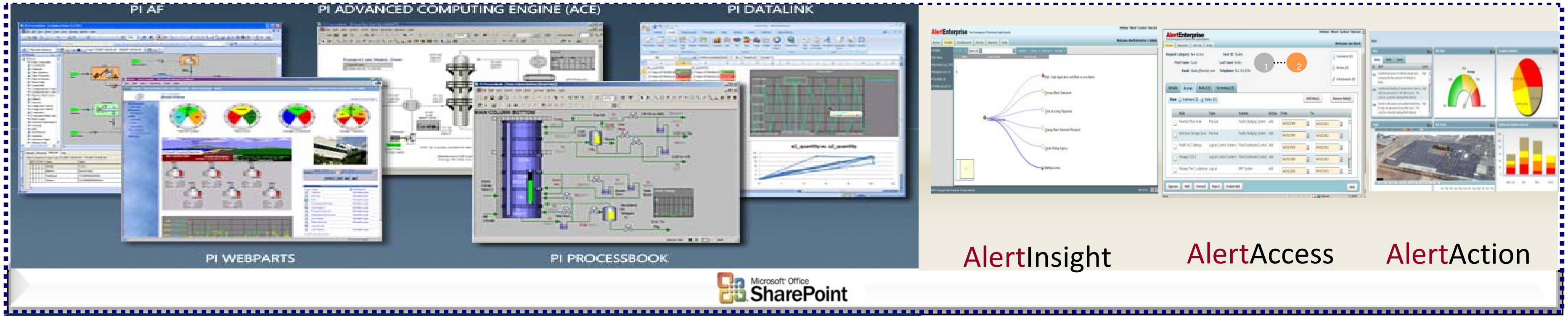
Toronto Hydro: Smart Grid Security Pilot

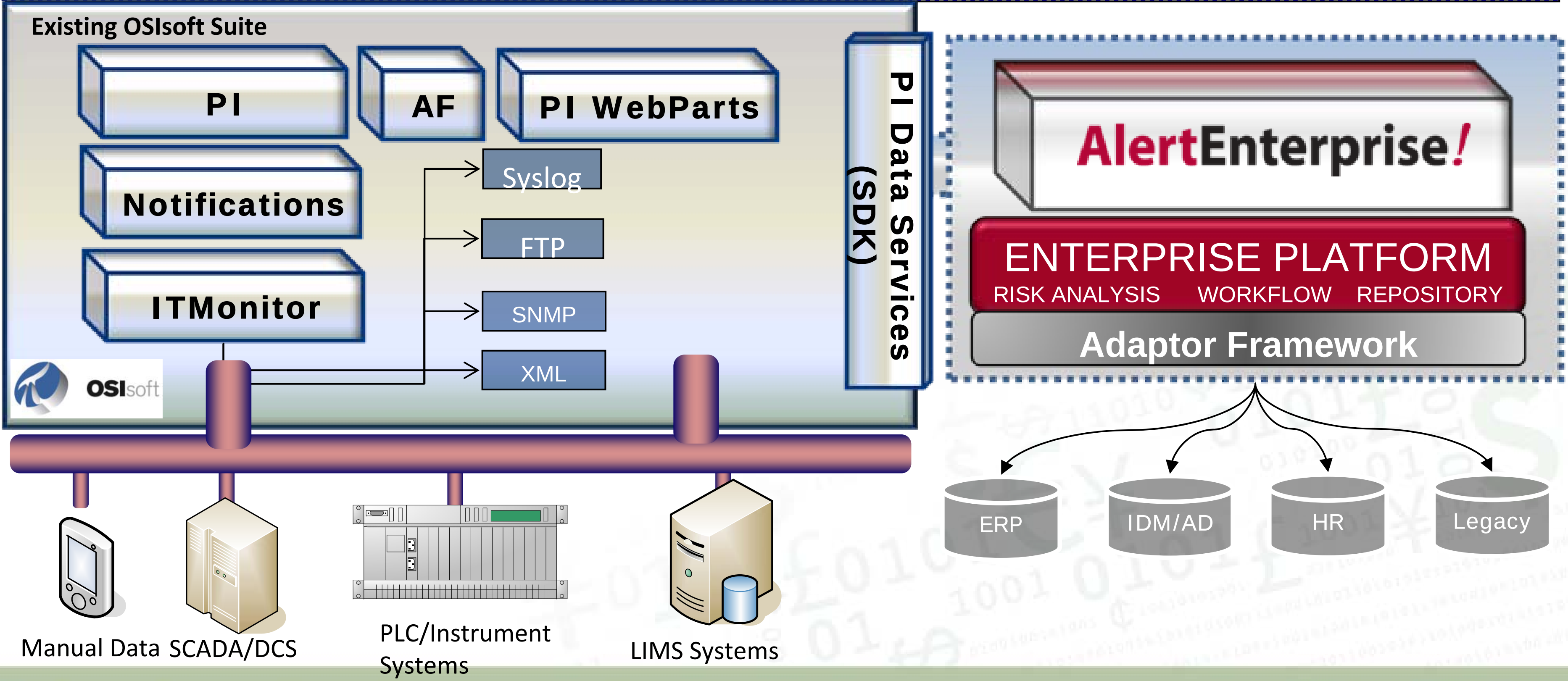
- ❖ Uncover blended threats across IT Systems, PACS and Industrial Controls
- ❖ Connect to the business systems like Oracle and SAP to aggregate IT access events and employee / contractor background and certification checks.
- ❖ Link to the PACS (badge system) and the video surveillance camera systems
- ❖ Leveraging the OSIsoft PI System, AlertEnterprise can correlate the above information with events, configuration changes and alerts from control system applications without impacting their performance.



Toronto Hydro Smart Grid Security Pilot

Solution Architecture (OSIsoft Integration)

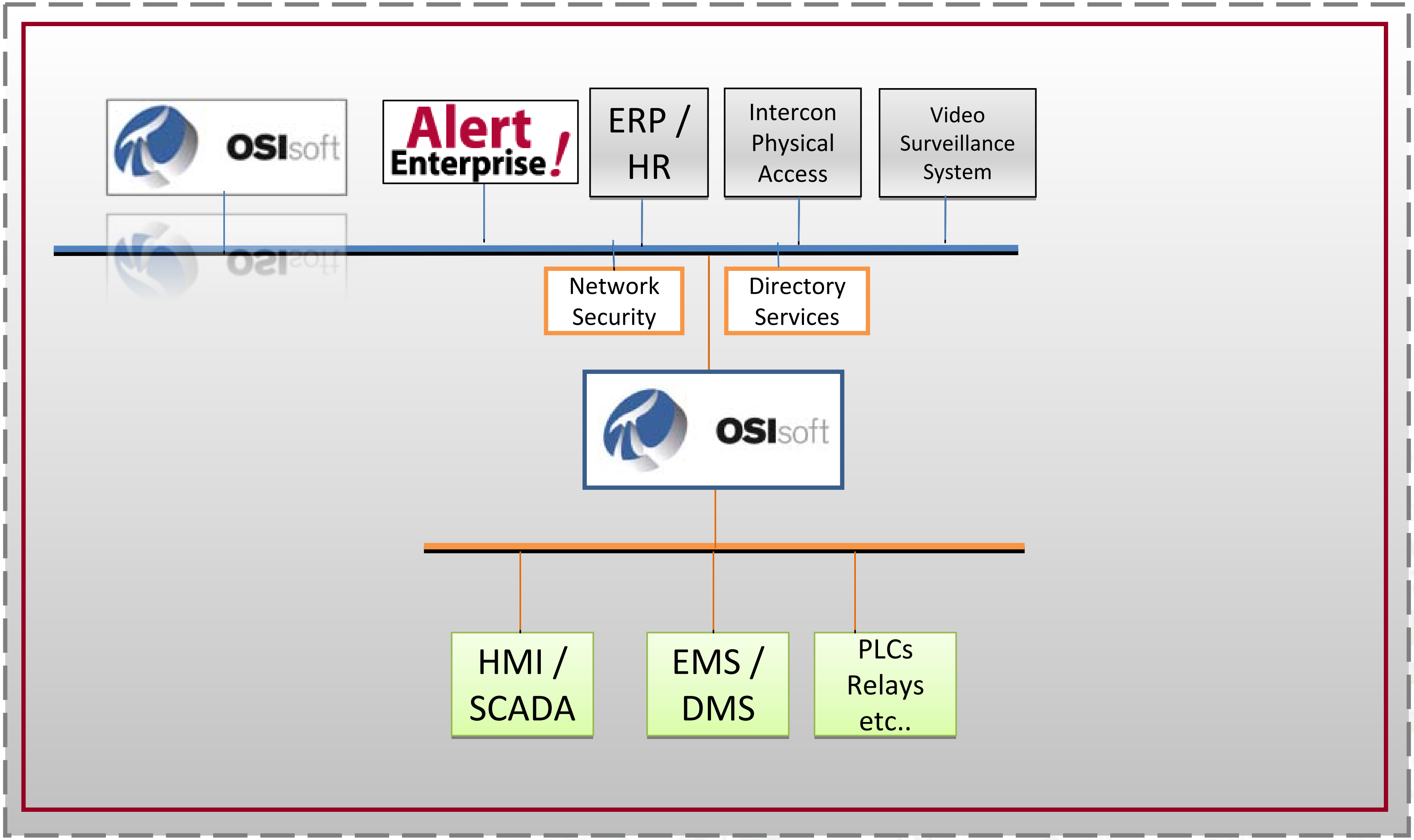




OSIsoft Provides the Conduit to the Real-Time Applications

- Non-invasive access to time-sequenced data from real-time applications - DCS, EMS, DMS, SCADA/HMI etc.
- Additional tags populated in the OSIsoft PI System for security configuration
- Combined with AlertEnterprise software OSIsoft Information can be correlated with ERP and Enterprise Applications
- For organizations who drive to optimize demand and supply, a mirror OSIsoft installation may be required on the corporate network

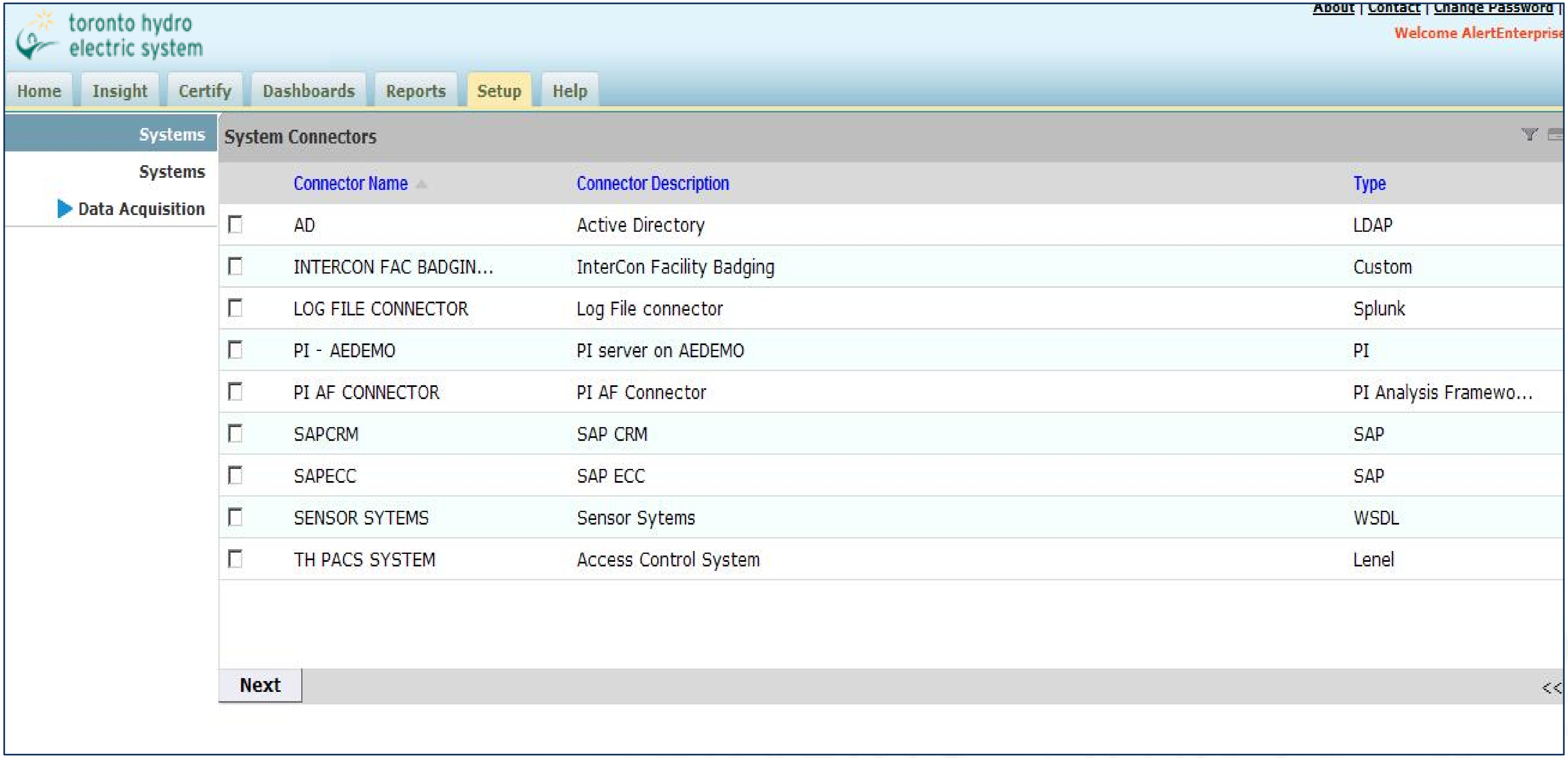
Maximizing Efficiency for the Real-Time Enterprise



Deployment

- CONFIGURING TO ORGANIZATIONAL SYSTEMS
- ENABLING FULL INTEGRATION WITH OSISOFT SYSTEMS
- CONNECTION TO PI NOTIFICATION
- SUBSCRIBING TO REQUESTS

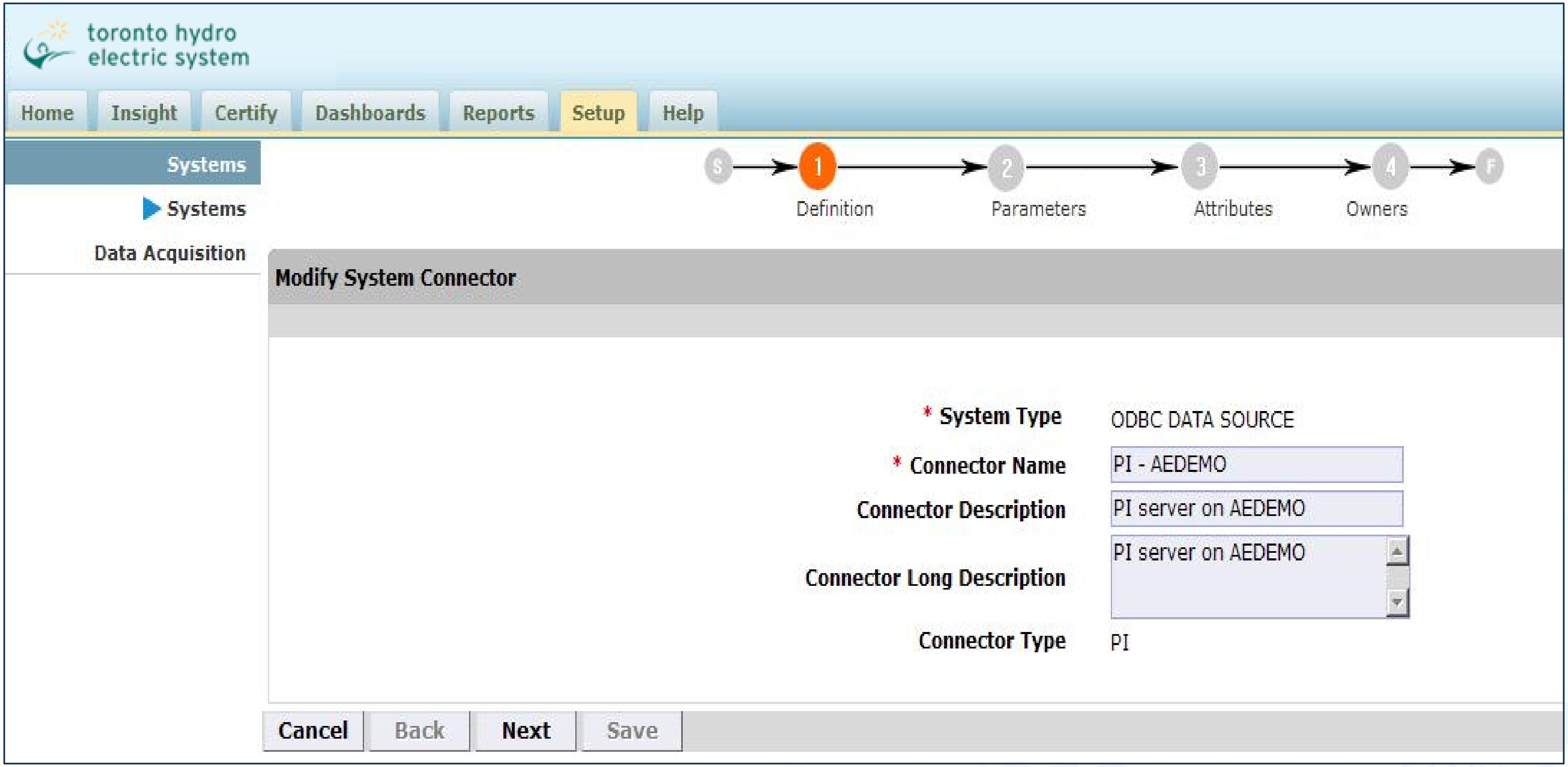
Connecting to Multiple Systems



System Connectors

	Connector Name	Connector Description	Type
□	AD	Active Directory	LDAP
□	INTERCON FAC BADGIN...	InterCon Facility Badging	Custom
□	LOG FILE CONNECTOR	Log File connector	Splunk
□	PI - AEDEMO	PI server on AEDEMO	PI
□	PI AF CONNECTOR	PI AF Connector	PI Analysis Framewo...
□	SAPCRM	SAP CRM	SAP
□	SAPECC	SAP ECC	SAP
□	SENSOR SYTEMS	Sensor Sytems	WSDL
□	TH PACS SYSTEM	Access Control System	Lenel

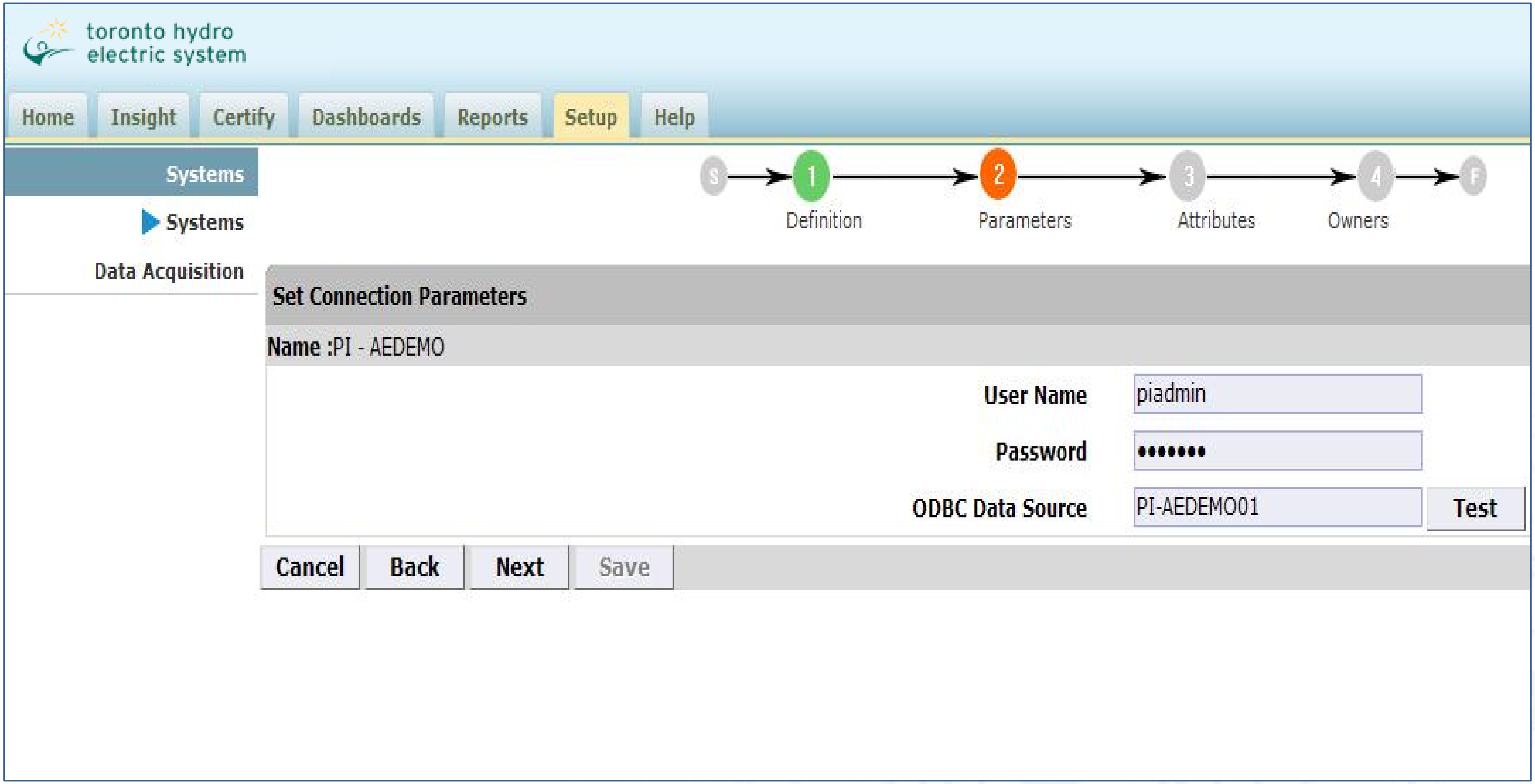
Configuring a Data Source



Modify System Connector

* System Type	ODBC DATA SOURCE
* Connector Name	PI - AEDEMO
Connector Description	PI server on AEDEMO
Connector Long Description	PI server on AEDEMO
Connector Type	PI

Configuring Connection to PI Notifications

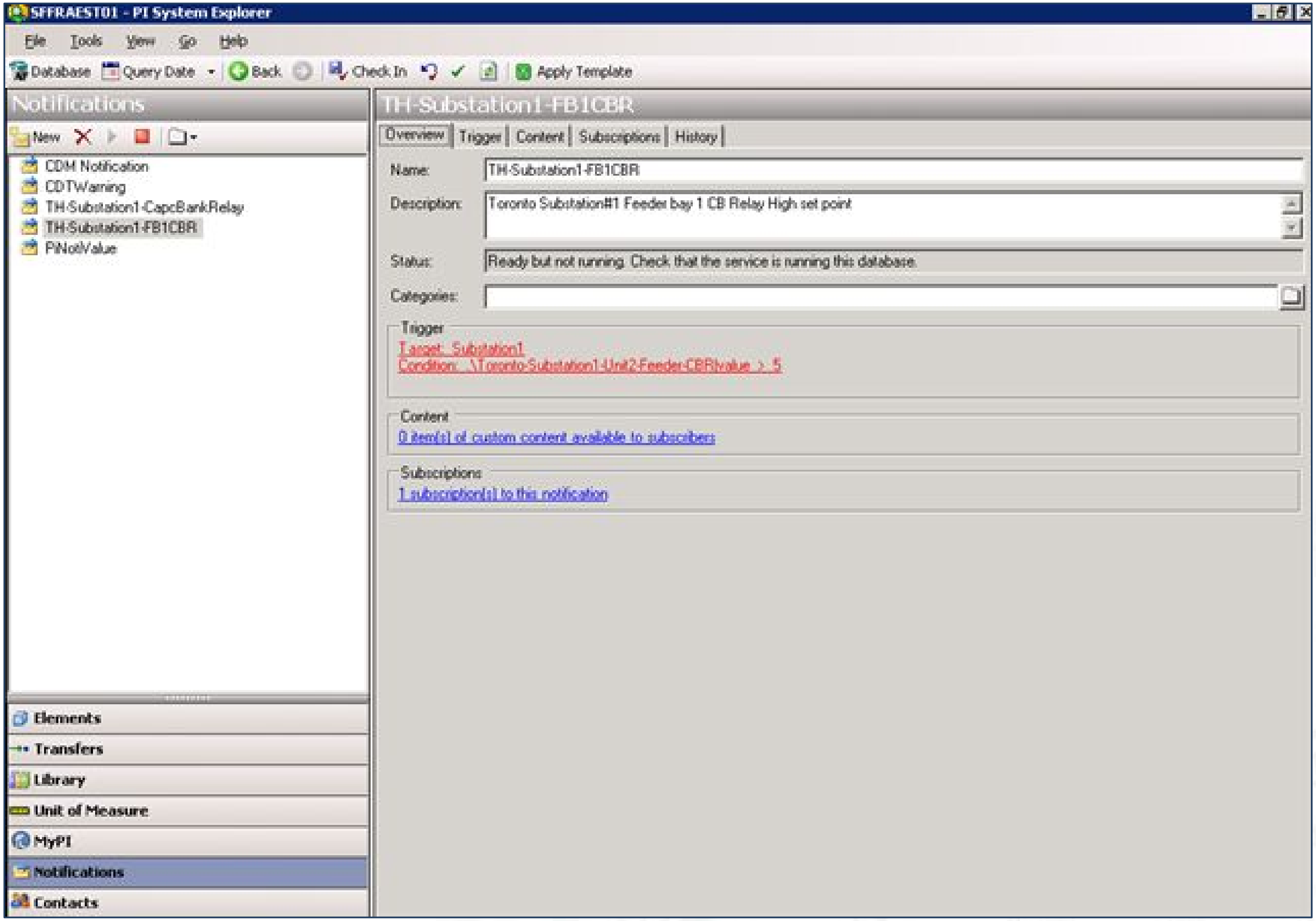


Set Connection Parameters

Name :PI - AEDEMO

User Name	piadmin
Password	•••••••
ODBC Data Source	PI-AEDEMO01

Trigger set in PI to monitor Set Point



Name: TH-Substation1-FB1CBR

Description: Toronto Substation#1 Feeder bay 1 CB Relay High set point

Status: Ready but not running. Check that the service is running this database.

Categories:

Trigger

Target: Substation1

Condition: .\Toronto-Substation1-Unit2-Feeder-CBR|value > 5

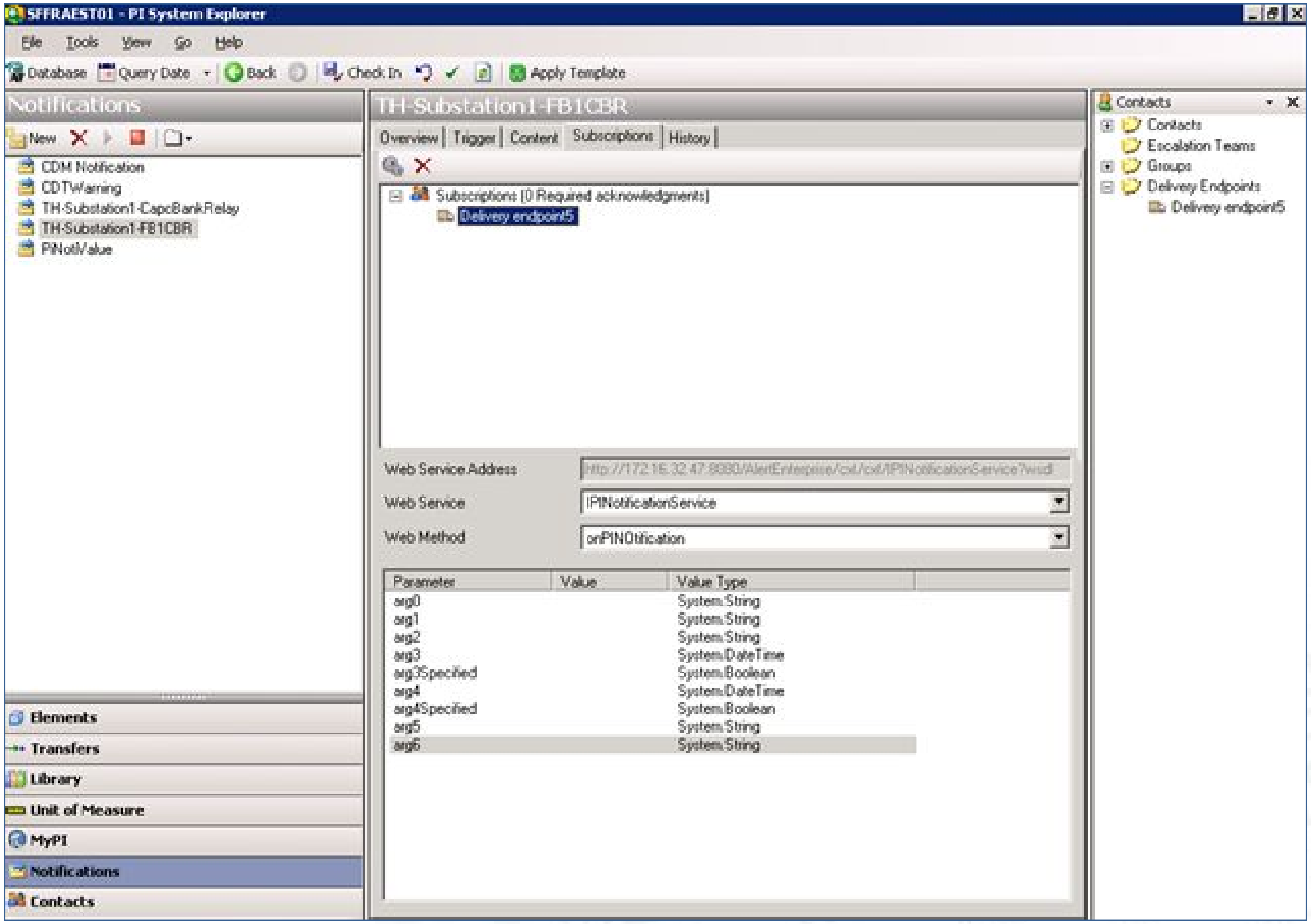
Content

0 item(s) of custom content available to subscribers

Subscriptions

1 subscription(s) to this notification

PI System Alerts Setup to Include AlertEnterprise



Web Service Address: http://172.16.32.47:8080/AlertEnterprise/cxf/cxf/IPINotificationService?wsdl

Web Service: IPINotificationService

Web Method: onPINOtification

Parameter	Value	Value Type
arg0		System.String
arg1		System.String
arg2		System.String
arg3		System.DateTime
arg3Specified		System.Boolean
arg4		System.DateTime
arg4Specified		System.Boolean
arg5		System.String
arg6		System.String

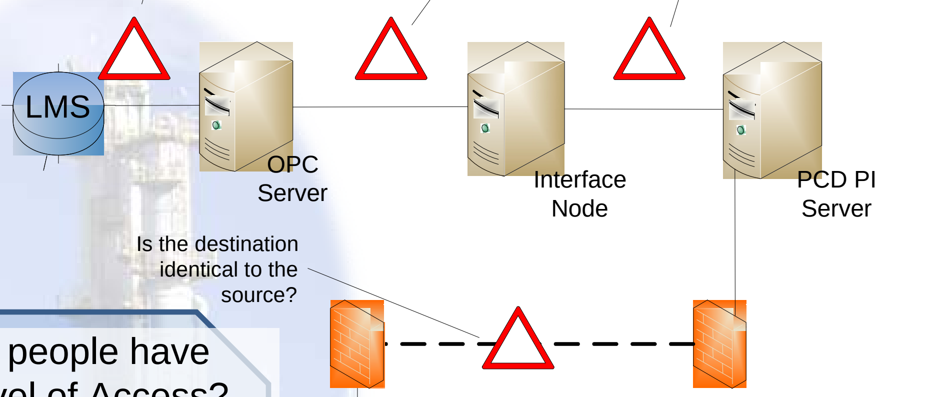
Monitoring Threshold Changes to PI Tag Data

TH-Substation1-FB1CBR	00:00.0	59.995	0
TH-Substation1-FB1CBR	00:00.1	59.993	0
TH-Substation1-FB1CBR	00:00.1	59.993	0
TH-Substation1-FB1CBR	00:00.1	59.997	0
TH-Substation1-FB1CBR	00:00.2	59.999	0
TH-Su			
TH-Su			
TH-Su			
TH-Su			
TH-Su			
TH-Su			
TH-Su			
TH-Su			
TH-Su			
TH-Su			
TH-Su			
TH-Su			
TH-Su			
TH-Substation1-FB1CBR	00:00.6	77.001	0
TH-Substation1-FB1CBR	00:00.7	76.996	0
TH-Substation1-FB1CBR	00:00.7	76.995	0
TH-Substation1-FB1CBR	00:00.7	76.997	0
TH-Substation1-FB1CBR	00:00.8	76.991	0
TH-Substation1-FB1CBR	00:00.8	76.992	0
TH-Substation1-FB1CBR	00:00.8	76.995	0
TH-Substation1-FB1CBR	00:00.9	76.996	0
TH-Substation1-FB1CBR	00:00.9	76.996	0
TH-Substation1-FB1CBR	00:00.9	76.998	0
TH-Substation1-FB1CBR	00:01.0	76.996	0
TH-Substation1-FB1CBR	00:01.0	77	0
TH-Substation1-FB1CBR	00:01.0	76.995	0
TH-Substation1-FB1CBR	00:01.1	76.994	0
TH-Substation1-FB1CBR	00:01.1	76.995	0

TH-Substation1-FB1CBR	00:00.6	59.993
TH-Substation1-FB1CBR	00:00.6	59.997
TH-Substation1-FB1CBR	00:00.6	77.001
TH-Substation1-FB1CBR	00:00.7	76.996
TH-Substation1-FB1CBR	00:00.7	76.995

AlertEnterprise integrates security into the process

- Do the people have right level of Access?
- Is the authorization being certified by someone?
- Do you know - who changed the set point value? And was it authorized?
- Are the Privileged Users being watched?

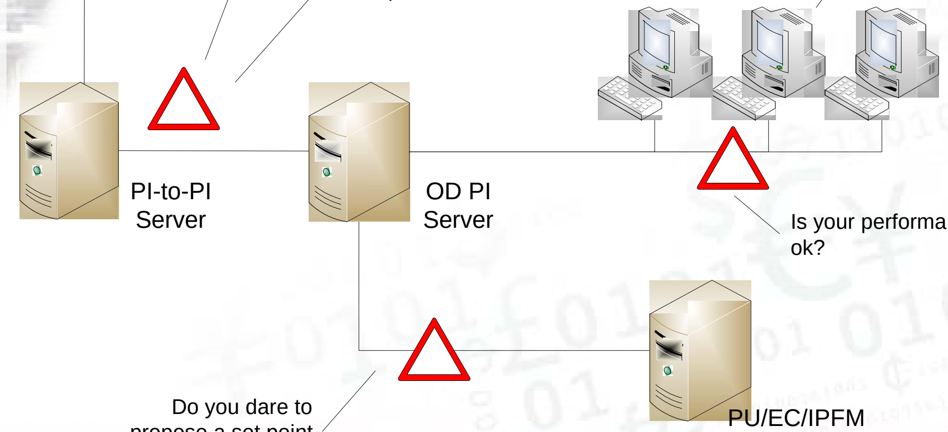


Are your transmitters calibrated?

Is the configuration right?

Is your network ok?

Is the destination identical to the source?

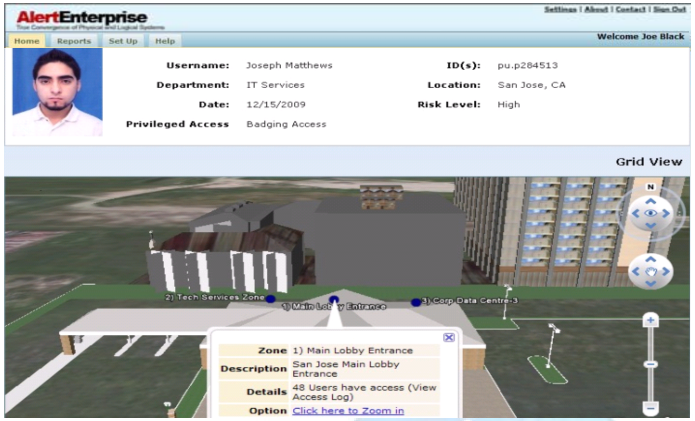


Is this a good quality value?

Is the current value really the one from the process?

Is your performance ok?

Do you dare to propose a set point value?



Username: Joseph Matthews

ID(s): pu.p284513

Department: IT Services

Location: San Jose, CA

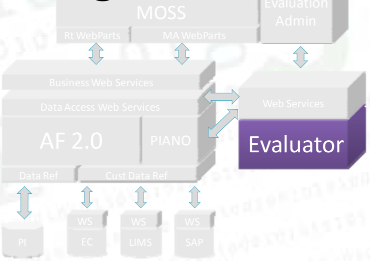
Date: 12/15/2009

Risk Level: High

Privileged Access Badging Access

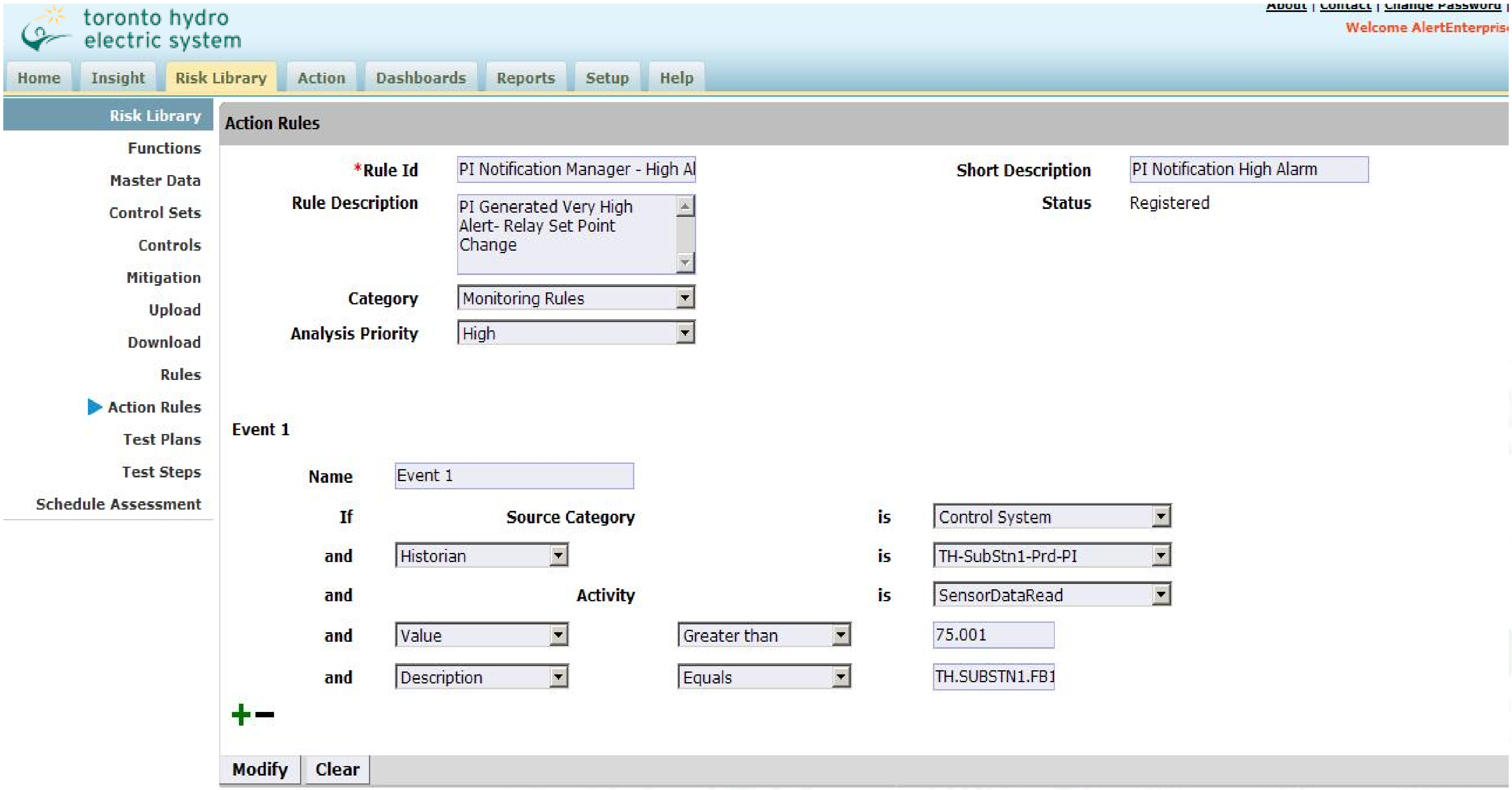
Zone	1) Main Lobby Entrance
Description	San Jose Main Lobby Entrance
Details	48 Users have access (View Access Log)
Option	Click here to Zoom in

Remote Login



Is access being monitored continuously?

Pre-configuring Rule Sets, Physical Configuration Screen, Configuring RAS



Action Rules

*Rule Id: PI Notification Manager - High Al

Short Description: PI Notification High Alarm

Rule Description: PI Generated Very High Alert- Relay Set Point Change

Status: Registered

Category: Monitoring Rules

Analysis Priority: High

Event 1

Name: Event 1

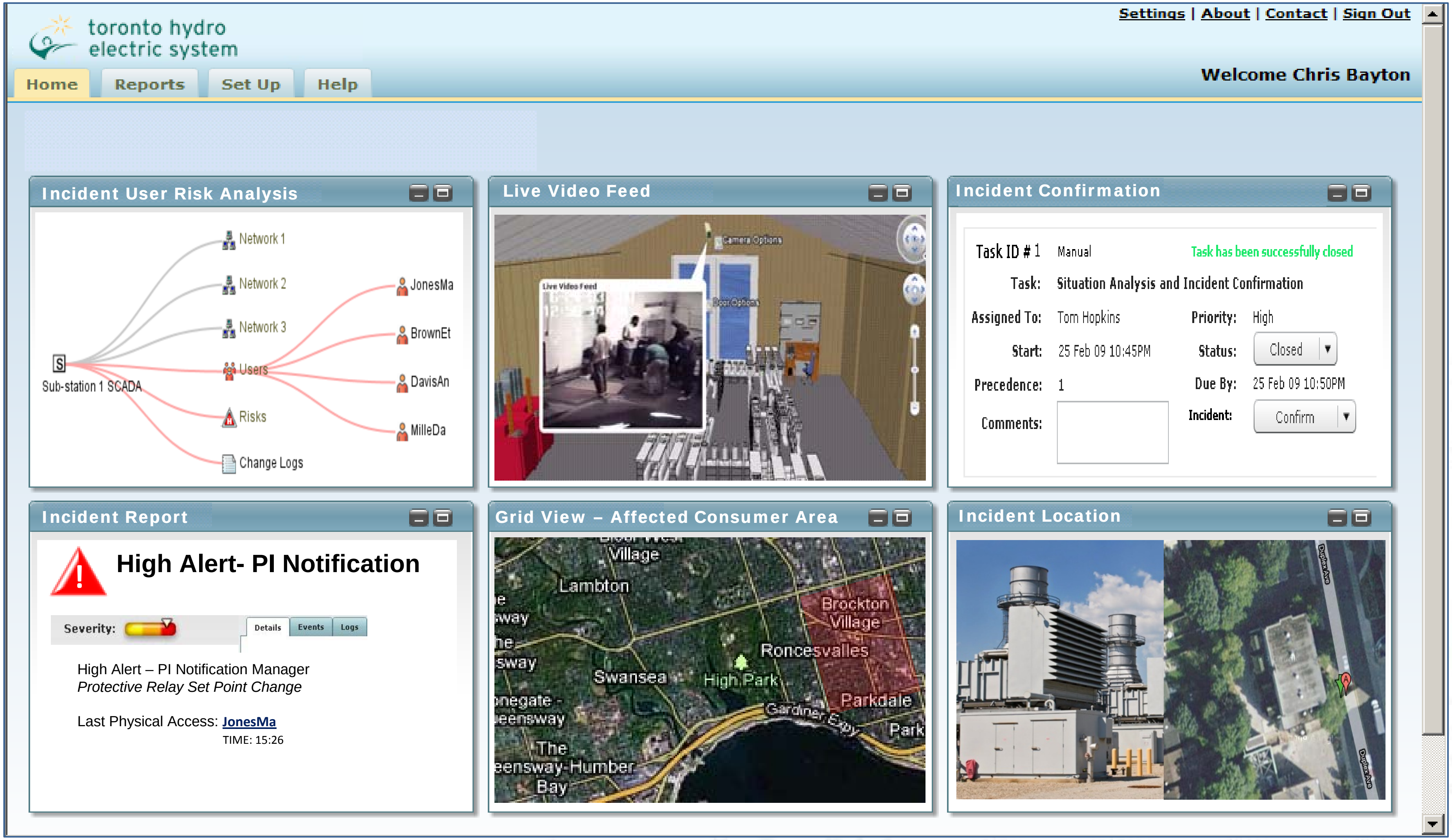
If		Source Category	is	Control System
and	Historian		is	TH-SubStn1-Prd-PI
and		Activity	is	SensorDataRead
and	Value	Greater than		75.001
and	Description	Equals		TH.SUBSTN1.FB1

+ −

Malicious Insider Scenario – Detect and Monitor

- Scenario: Attempt to shut down grid by disabling two levels of protective relays and defeating interlocks.
- Toronto Hydro Requirement
  - Identify and confirm incident
  - Initiate notification workflow
  - Invoke Geo-Spatial Monitoring
  - Initiate Lockdown Sequence
  - Notify first responders for dispatch

Toronto Hydro: Converged Dashboard


toronto hydro electric system
Settings | About | Contact | Sign Out
Home
Reports
Set Up
Help

Welcome Chris Bayton

Incident User Risk Analysis

Live Video Feed

Incident Confirmation

Task ID # 1 Manual Task has been successfully closed

Task: Situation Analysis and Incident Confirmation

Assigned To: Tom Hopkins Priority: High

Start: 25 Feb 09 10:45PM Status: Closed ▼

Precedence: 1 Due By: 25 Feb 09 10:50PM

Comments: Incident: Confirm ▼

Incident Report

High Alert- PI Notification

Severity:

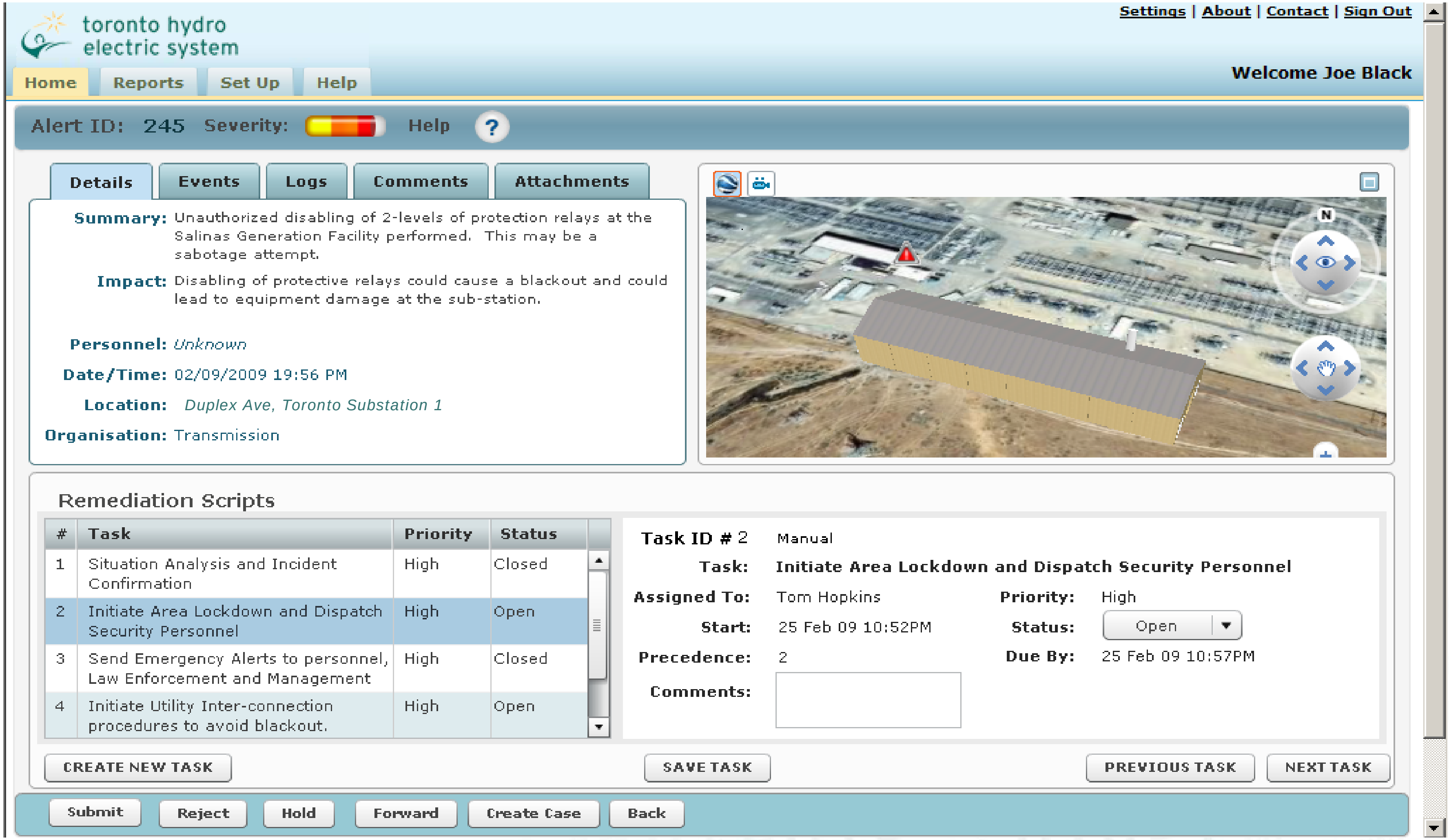
High Alert – PI Notification Manager
Protective Relay Set Point Change

Last Physical Access: JonesMa
TIME: 15:26

Grid View – Affected Consumer Area

Incident Location

Geo-spatial View Of Substation



Alert ID: 245 Severity:

Summary: Unauthorized disabling of 2-levels of protection relays at the Salinas Generation Facility performed. This may be a sabotage attempt.

Impact: Disabling of protective relays could cause a blackout and could lead to equipment damage at the sub-station.

Personnel: *Unknown*

Date/Time: 02/09/2009 19:56 PM

Location: *Duplex Ave, Toronto Substation 1*

Organisation: Transmission

Remediation Scripts

#	Task	Priority	Status
1	Situation Analysis and Incident Confirmation	High	Closed
2	Initiate Area Lockdown and Dispatch Security Personnel	High	Open
3	Send Emergency Alerts to personnel, Law Enforcement and Management	High	Closed
4	Initiate Utility Inter-connection procedures to avoid blackout.	High	Open

Task ID # 2 Manual

Task: **Initiate Area Lockdown and Dispatch Security Personnel**

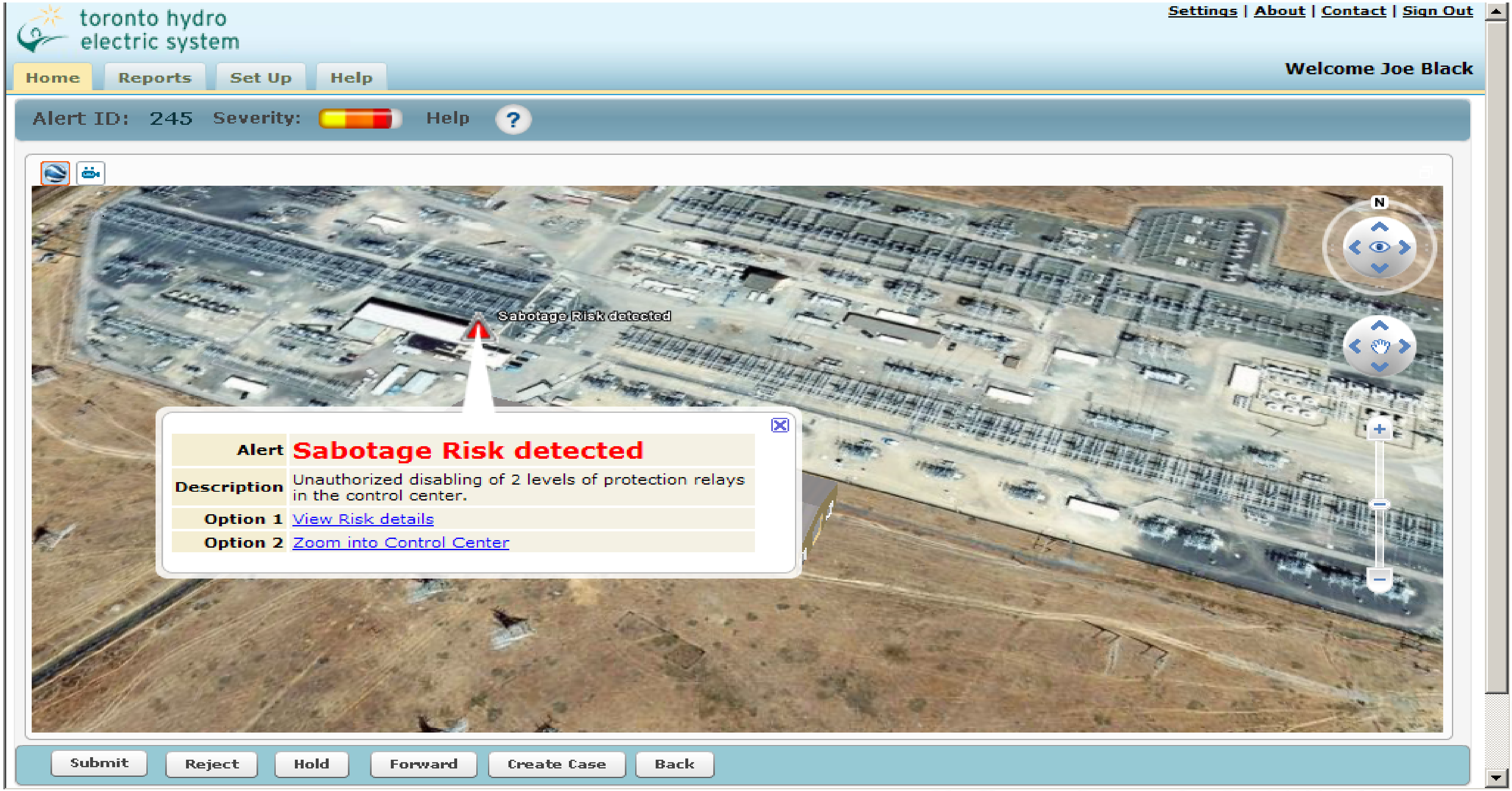
Assigned To: Tom Hopkins **Priority:** High

Start: 25 Feb 09 10:52PM **Status:** Open

Precedence: 2 **Due By:** 25 Feb 09 10:57PM

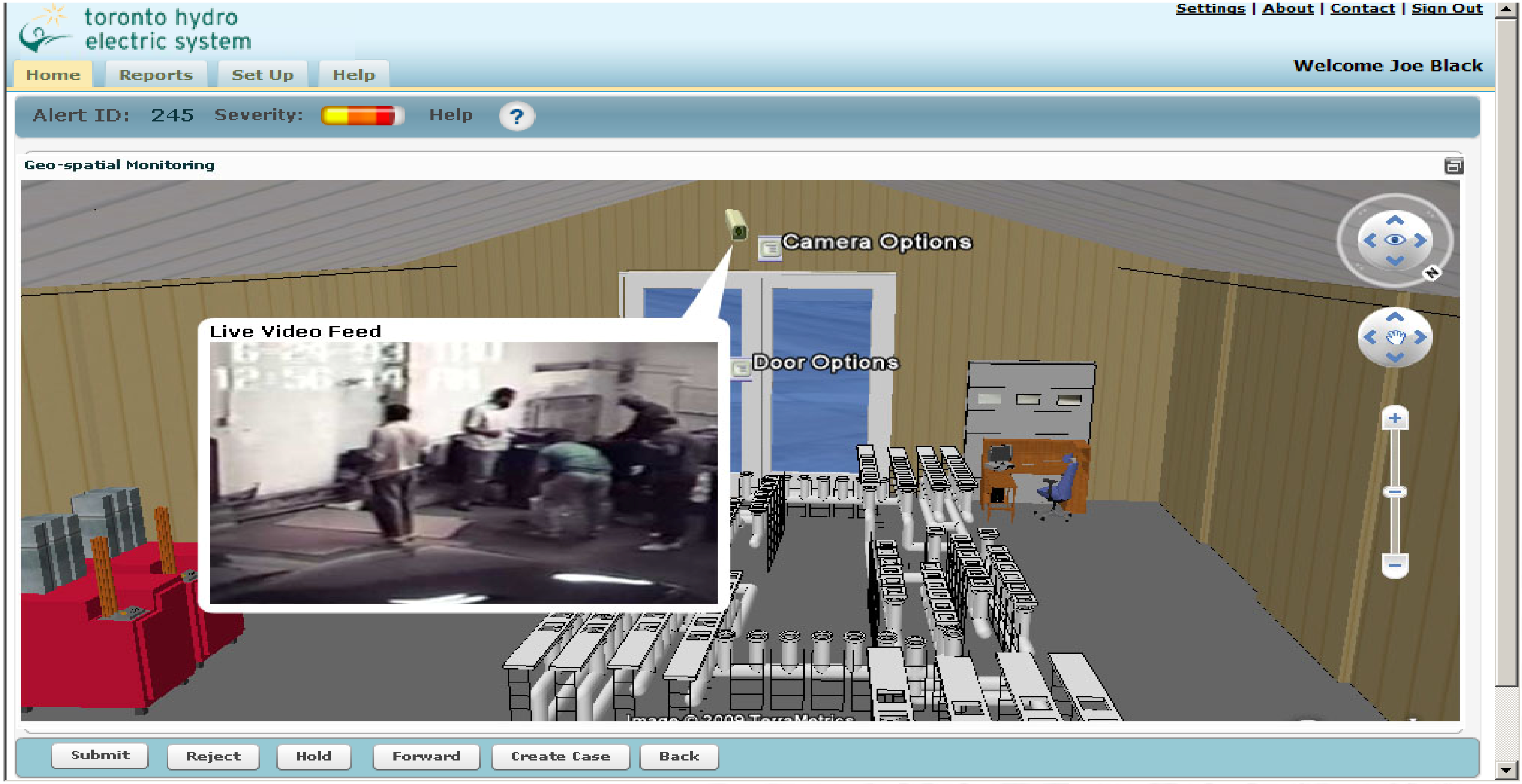
Comments:

Substation – Sabotage Risk!



Alert	Sabotage Risk detected
Description	Unauthorized disabling of 2 levels of protection relays in the control center.
Option 1	View Risk details
Option 2	Zoom into Control Center

Access Live Video & Initiate Physical Lockdown



Welcome Joe Black

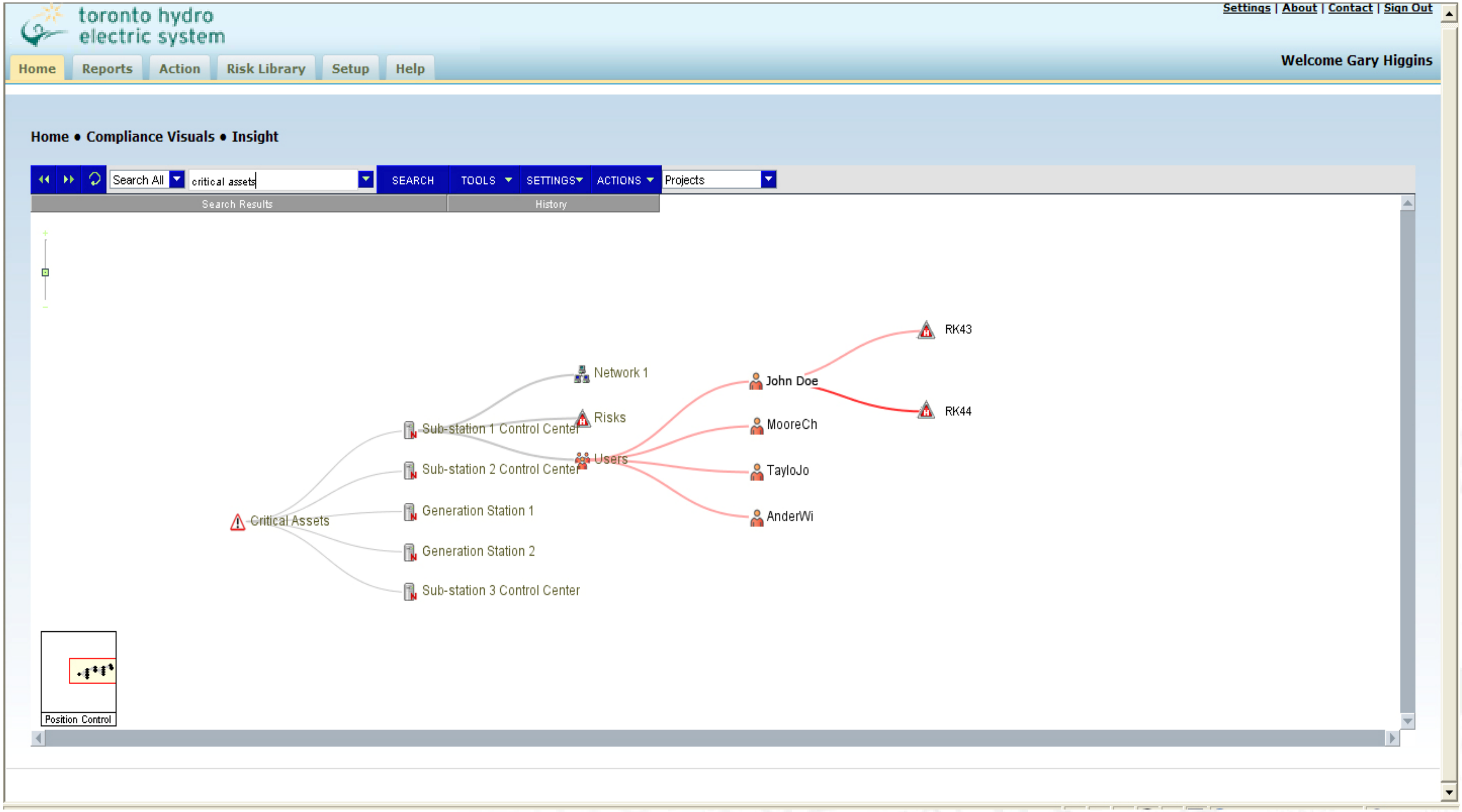
Alert ID: 245 Severity:

Identifying Users Associated with Critical Change

- Scenario: John has privileged physical and control system access to conduct a critical change.

- Toronto Hydro Requirements:
  - Conduct Correlative Risk Analysis Across IT Applications, Physical Access Systems, And Control System Operation
  - Assign Mitigation Controls
  - Generate Alerts, Investigate, Respond, & Revoke Access in Real-Time to reduce property or human loss

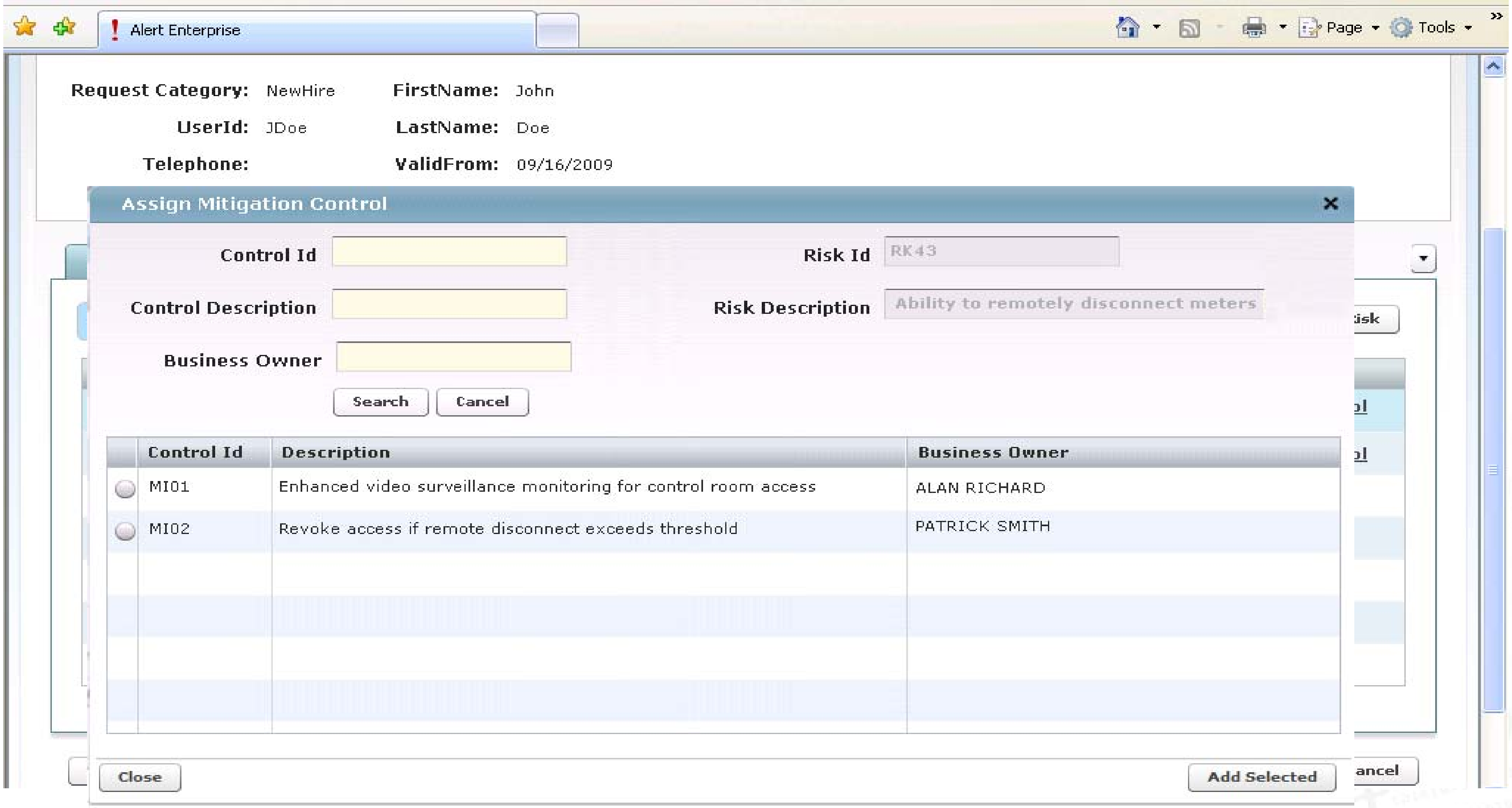
Identifying Threat Scenario Visually



Welcome Gary Higgins

Home • Compliance Visuals • Insight

Access Risks Identified, Mitigated



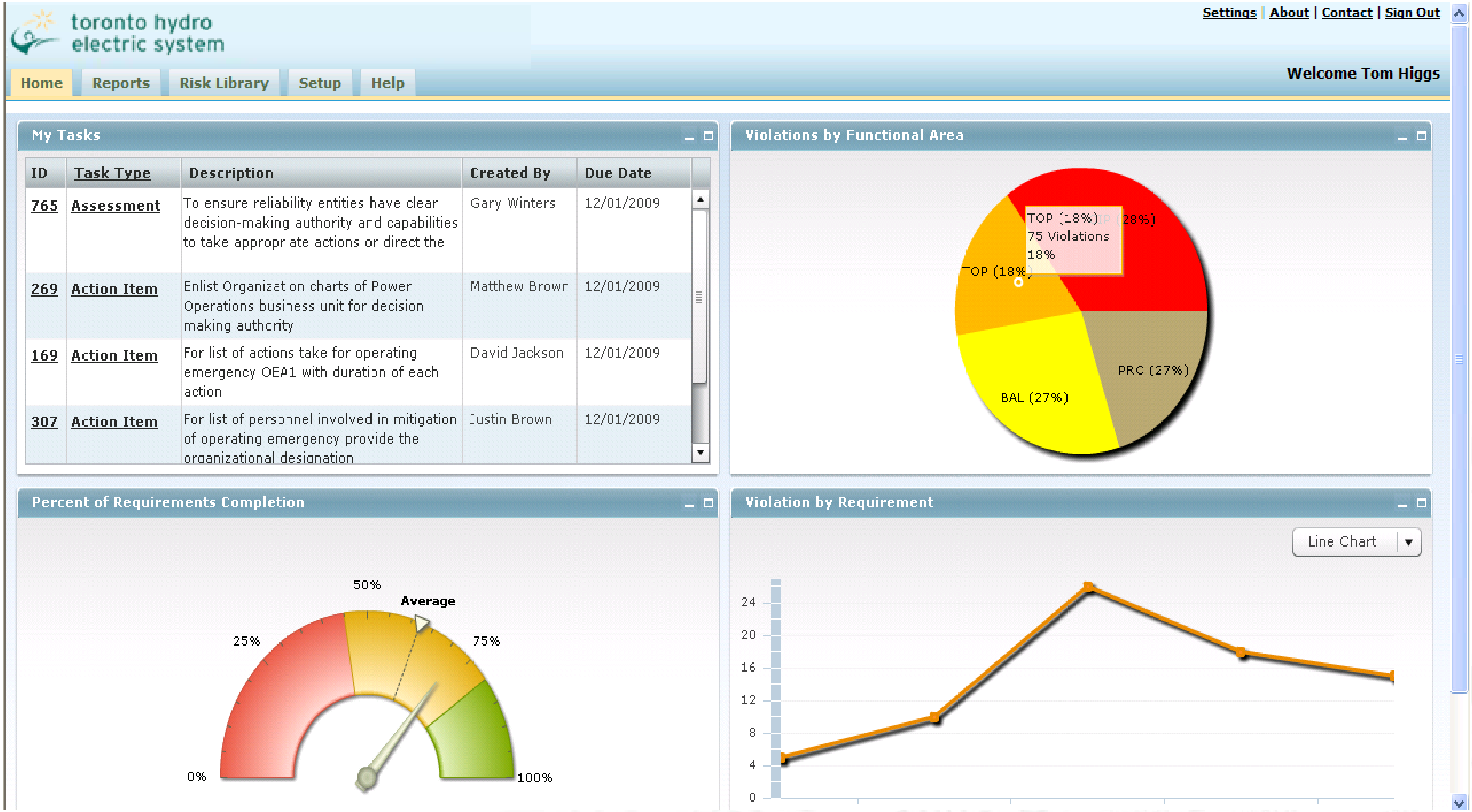
Request Category:	NewHire	FirstName:	John
UserId:	JDoe	LastName:	Doe
Telephone:		ValidFrom:	09/16/2009

Assign Mitigation Control

Control Id		Risk Id	RK43
Control Description		Risk Description	Ability to remotely disconnect meters
Business Owner			

	Control Id	Description	Business Owner
○	MI01	Enhanced video surveillance monitoring for control room access	ALAN RICHARD
○	MI02	Revoke access if remote disconnect exceeds threshold	PATRICK SMITH

Monitoring Progress of Security & Compliance Initiatives



toronto hydro electric system

Settings | About | Contact | Sign Out

Home | Reports | Risk Library | Setup | Help

Welcome Tom Higgs

My Tasks

ID	Task Type	Description	Created By	Due Date
765	Assessment	To ensure reliability entities have clear decision-making authority and capabilities to take appropriate actions or direct the	Gary Winters	12/01/2009
269	Action Item	Enlist Organization charts of Power Operations business unit for decision making authority	Matthew Brown	12/01/2009
169	Action Item	For list of actions take for operating emergency OEA1 with duration of each action	David Jackson	12/01/2009
307	Action Item	For list of personnel involved in mitigation of operating emergency provide the organizational designation	Justin Brown	12/01/2009

Violations by Functional Area

Percent of Requirements Completion

Violation by Requirement

Line Chart ▾

Continuous Program for Security, Risk and Compliance Delivers Value

- Integration with OSIsoft PI enables organizations to extend risk analysis to real-time control system information
- Continuous compliance processes are sustainable and can adopt to emerging regulations, organizational policies
- Accommodate new security demands created by Smart Grid deployments
- Contain costs for audit and compliance
- Reduce Bottom Line Cost, Streamline Operational Processes

OSIsoft® UC 2010

Real Time Information — Currency of the New Decade

Thank you