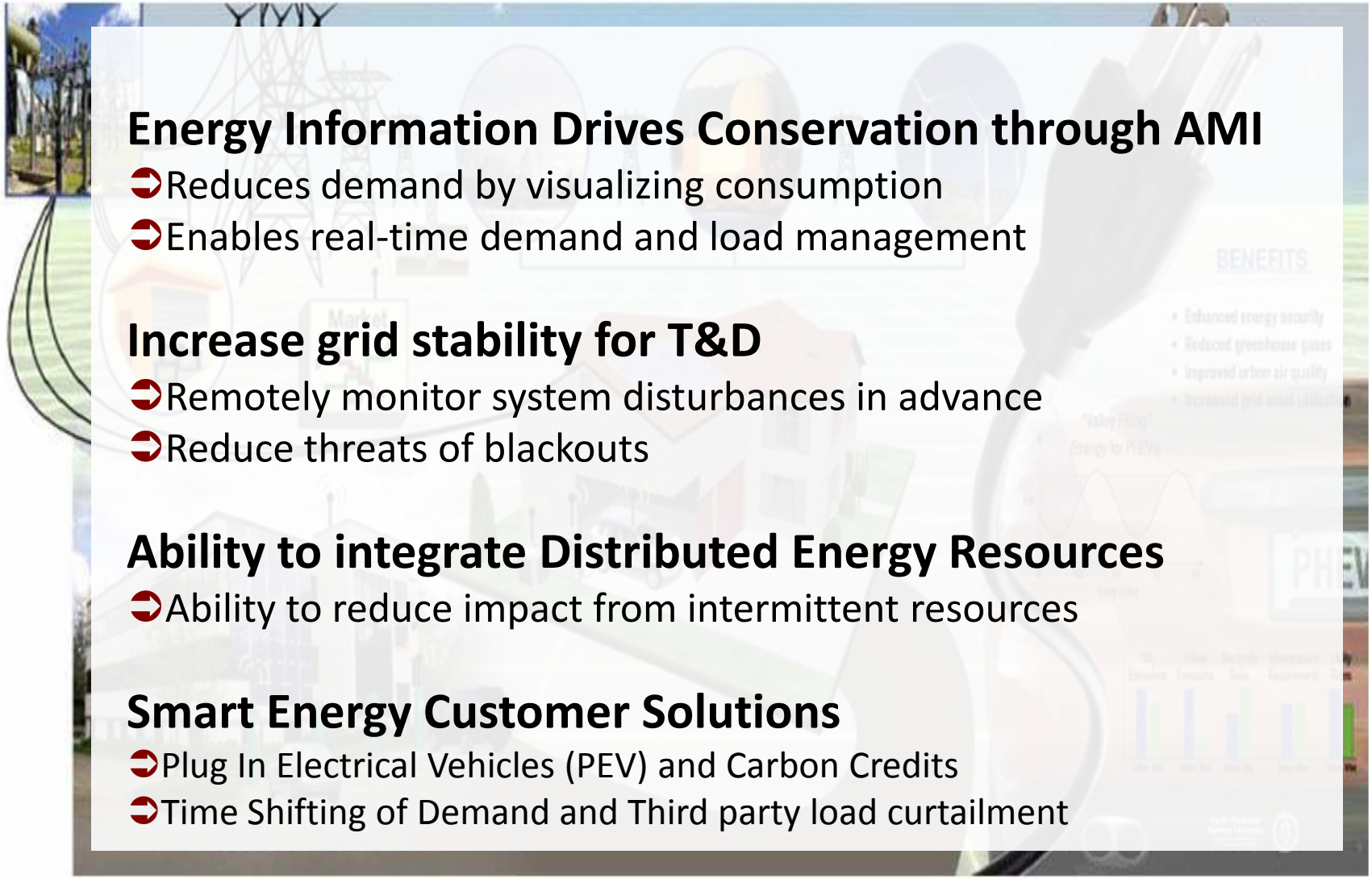
Security Convergence for the Smarter Grid

Kshamit Dixit CISM, MBA, MS (Eng)
Manager, IT Security
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

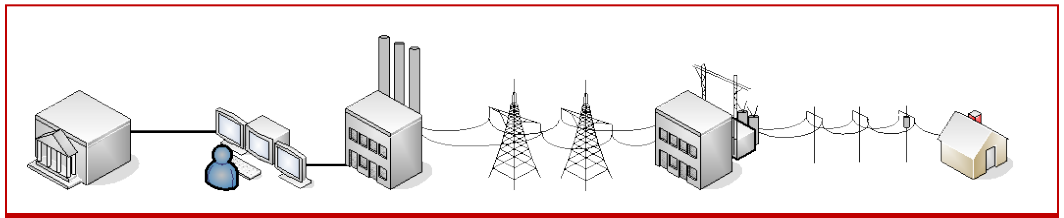
Smart Grid Poses New Challenges

- 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…

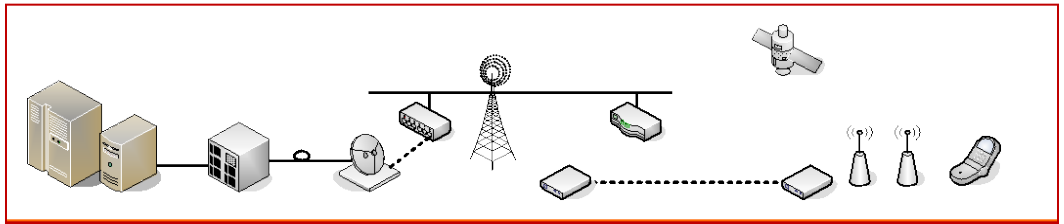
Traditional Threats, Risks, Security Challenges for Utilities

- 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)

Smart Grid is driving the integration of two infrastructures…



Electrical infrastructure



Information infrastructure

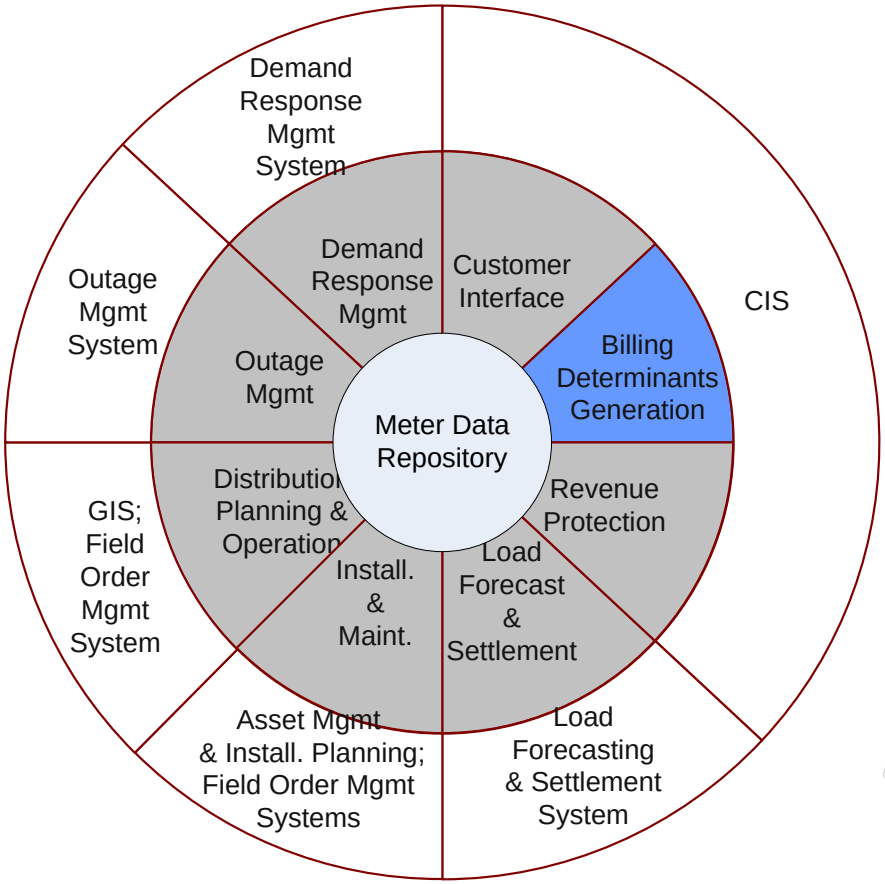
- Integration between plant operations and business
- Real-time monitoring for power quality and reliability
- Demand and consumption monitoring
- Integrating alternative energy sources

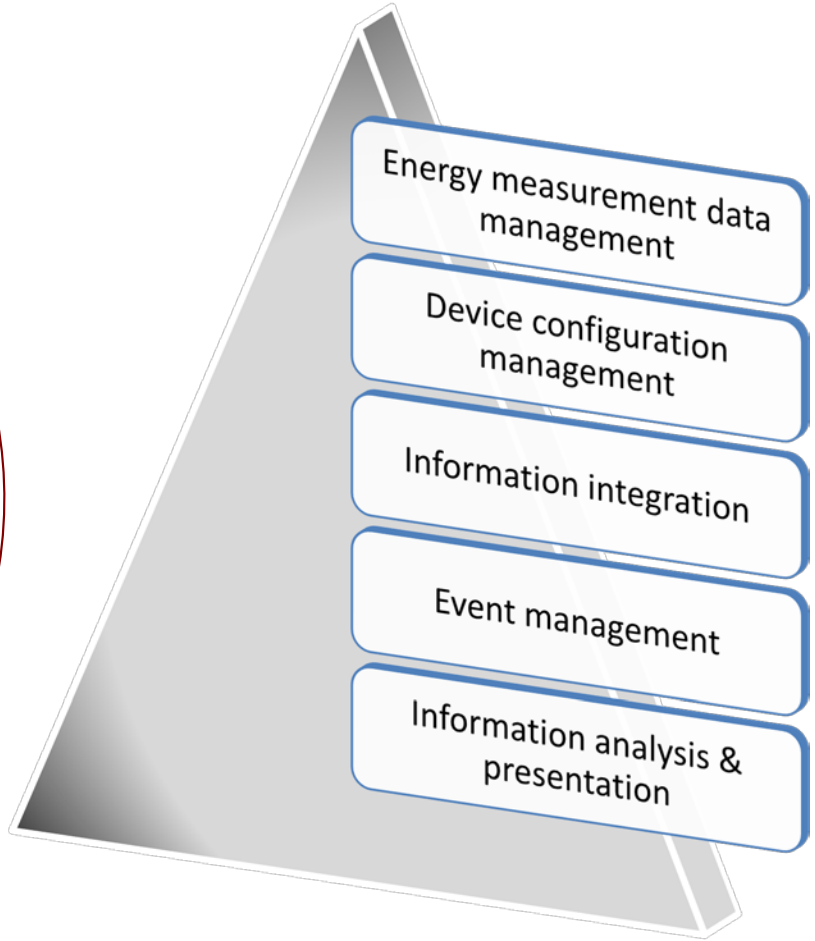
Securing these combined infrastructures requires a new approach to security that addresses blended threats through the convergence of IT Security, Physical Access Security and Control System Security.

Smart Grid Cyber Security Issues

- Need to protect Time of Use (TOU) data from non-authorized users
- Need to protect meters from being abused as control channel into grid operations
- Need to protect future two-way communications for meter activity
- Need to ensure future control capability is secure

The Power of Integration





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.

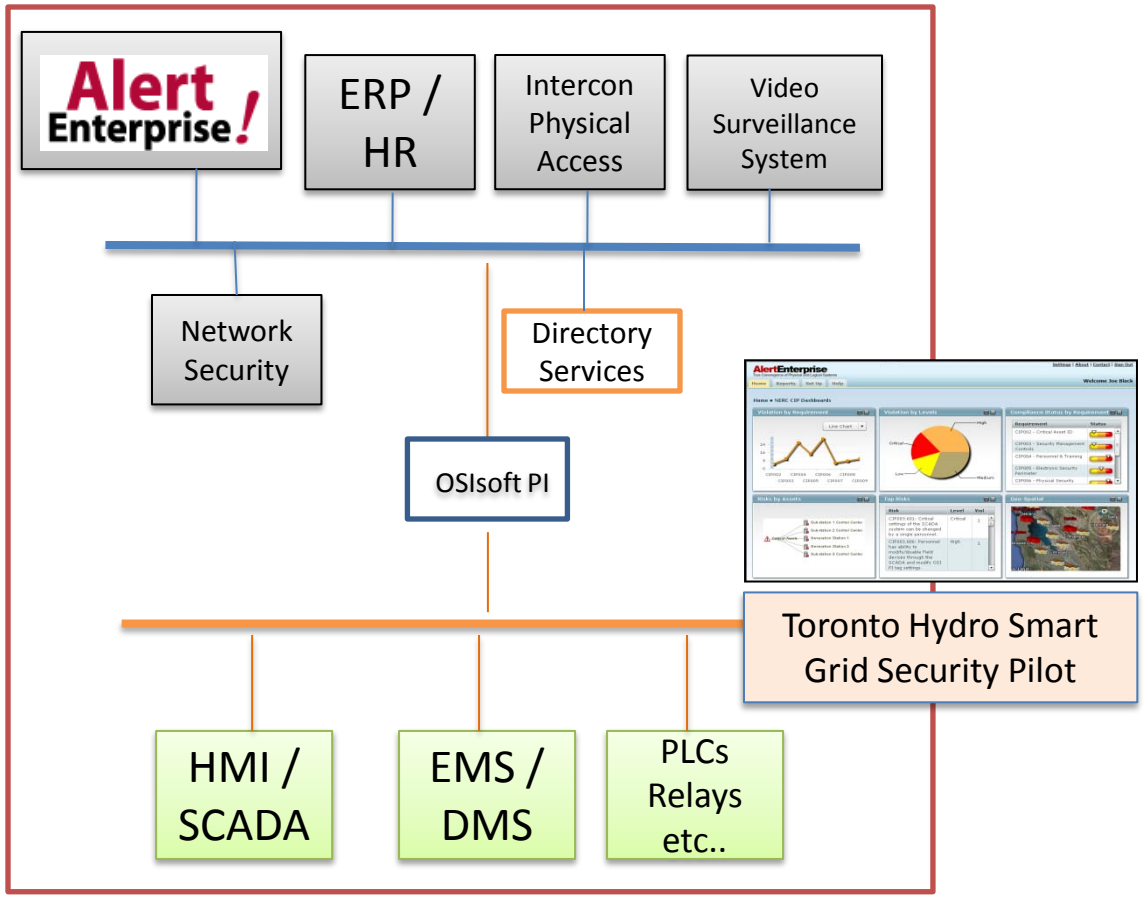
Active Policy Enforcement Scenario

- **Prescribed Policy**: Changes to Control System Settings must be Monitored. Privileged Users (Control Room Operators) must be authenticated prior to SCADA configuration changes being accepted.

- **Active Policy Enforcement Solution**: AlertEnterprise software is configured to monitor threshold value changes in OSIsoft PI historian logging SCADA activity and create an alert when an operator makes any requests to view or monitor critical assets. Following that record an event and automatically deliver a live video feed from the surveillance system allowing operations or security managers to remotely authenticate the changes.

Toronto Hydro Smart Grid Security Pilot

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



Continuous Program for Security, Risk and Compliance Delivers Value

- Incorporate Risk-based approach to security
- Next generation technology makes reviewing security risks more business-friendly
- Continuous compliance processes are sustainable and can adopt to emerging regulations, cultural policies
- Accommodate new security demands created by Smart Grid deployments
- Contain costs for audit and compliance
- Reduce Bottom Line Cost, Streamline Operational Processes

Thank You

Kshamit Dixit
KDixit@torontohydro.com