Debunking the Myths of SCADA Security
Jasvir Gill
CEO, AlertEnterprise
Which way is CIP Stretching You?
**SCADA/Control Engineers Are from MARS and IT Security is from Venus**

<table>
<thead>
<tr>
<th>SCADA, EMS, DMS and Control Systems Security</th>
<th>Systems, Applications and IT Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control system events and alerts must captured in real-time</td>
<td>Events are usually persisted in a database for action</td>
</tr>
<tr>
<td>Not originally designed with security in mind</td>
<td>Security culture and access controls designed into process</td>
</tr>
<tr>
<td>Large physical assets, remote systems, geographically dispersed</td>
<td>Controlled access in data centers</td>
</tr>
<tr>
<td>Conventional IT security tools – scanners etc. can shut down the plant</td>
<td>Depend on security technologies at various levels – perimeter, network, server, OS and application level security</td>
</tr>
</tbody>
</table>
Integration of Corporate and Plant Networks

Introduces Vulnerabilities

Corporate Network

SAP
Other ERP
HRMS
Web Servers

Supply Chain

CRM

Active Directory

Plant Network

OSIsoft Enterprise

DCS
HMI / SCADA
OSIsoft PI
LIMS
EMS / DMS
PLCs..
Complex Risks and Security Challenges

Threats

- Physical and Cyber protection of Sensitive Assets & Intellectual Property
- Sensitive Asset Diversion (Dangerous Chemicals, Pathogens, Nuclear material)
- Cyber Attacks - Utilities (Water, Power, Gas), Smart Grids, Transportation
- Terrorism (Chemicals stolen to make explosives)
- Bio Terrorism (Food & Beverage, Consumer Products)
- Disgruntled employees/contractors (both current and past)

Monitoring both Access and Behavior

- Do right people have access to assets (job, certifications, background)
- Any suspicious behavior or activities

Monitoring Privileged Users and “Access Creep” Industry Specific Compliance

- NERC, FERC, FISMA, PCI, HIPAA, CFATS, etc
Problem/Challenge:
Too many silos (inefficient, expensive, fraught with risk)

- Human resources
- Silos of user information
- Disjointed processes
- Inefficient
- Security gaps
- No preventive and comprehensive risk analysis
- Contractors
- Background Checks/Certification
- Assets
- Governance risk & compliance
- Cloud Security
- IT/ERP security
- Physical security
- Industry Specific Risk Library
- Internal Control Policies
- SCADA/Network
AlertEnterprise Solution:
Streamlines on-boarding/off-boarding & closes security gaps

Enterprise Compliance
Eliminate Overlaps
Workplace Efficiency
Simplify & automate onboarding & offboarding
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
NERC CIP and Other Compliance Solutions – Life in the Trenches Today

- Silo-ed approach and point-solution for each regulation
- Sustainability - Controls testing and audit functions duplicated for each regulation
- Control Documentation Solutions are not Integrated with ERP Systems.
- Integration of systems across the grid is creating privacy and data leakage scenarios.
- Manual testing of controls is painful, time consuming, error-prone and not scalable.
Even after all this – organizations are not secure enough and have not completely mitigated risk.

According to Michael Assante, Chief Security Officer, NERC -
“Compliance does not make you any more secure unless you have Active Policy Enforcement.”
Bridge the security gaps between IT, Physical and Control Systems

- Risk analysis across all three domains
- Detect, identify and eliminate risks before they manifest
- True prevention of threats from thefts, sabotage and terrorism
- Incident management with built-in programmed remediation
- Policy Based (Compliance to various regulations/policies)
Problem/Challenge:
Risk analysis too complex for non-technical staff

Can your business people find and fix risk in the following?
This is one of the major reasons for high TCO and lack of sustainability
### Request Number: 89

**Request Category:** Change Access

**User ID:** Matt

**First Name:** Matt

**Last Name:** Jones

**Email:** mattj@alert.com

**Telephone:** 510-323-1342

---

### My Systems

<table>
<thead>
<tr>
<th>System</th>
<th>Owner</th>
<th>Action</th>
<th>Valid From</th>
<th>Valid To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facility Badging System</td>
<td>Tom Smith</td>
<td>Change User</td>
<td>04/01/2009</td>
<td>04/02/2011</td>
</tr>
<tr>
<td>Transmission SCADA HMI</td>
<td>Jim Nelson</td>
<td>New User</td>
<td>04/01/2009</td>
<td>04/02/2009</td>
</tr>
<tr>
<td>OSISoft PI DB System</td>
<td>Gary Higgins</td>
<td>Change User</td>
<td>04/01/2009</td>
<td>04/02/2009</td>
</tr>
</tbody>
</table>
Alertinsight - Visualize Gaps And Automate Remediation
Alertinsight - Visualize Gaps And Automate Remediation
Alertinsight - Visualize Gaps And Automate Remediation

- Terminated users have active access to the SCADA system.
- SOARisk-Ability to modify relays through SCADA and change access to PI Historian.
- Critical configuration changes can be performed by a single user.
- Terminated users have active physical access to the SCADA system.
- Valid remote access to non-employees with admin privileges.
Solution – Converged Dashboard

Security & Compliance Portal

User Based Risk Analysis

Violation by Levels

Task ID # 1
Task: Situation Analysis and Incident Confirmation
Assigned To: Tom Hopkins
Start: 25 Feb 09 10:45PM
Status: Closed
Due By: 25 Feb 09 10:50PM
Precedence: 1
Priority: High
Comments: Task has been successfully closed
Incident: Confirm

Compliance Status by Requirement

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIP002 - Critical Asset ID</td>
<td>![Green Check]</td>
</tr>
<tr>
<td>CIP003 - Security Management Controls</td>
<td>![Green Check]</td>
</tr>
<tr>
<td>CIP004 - Personnel &amp; Training</td>
<td>![Green Check]</td>
</tr>
<tr>
<td>CIP005 - Electronic Security Perimeter</td>
<td>![Green Check]</td>
</tr>
<tr>
<td>CIP006 - Physical Security</td>
<td>![Green Check]</td>
</tr>
</tbody>
</table>

Well Trend

Top Risks

Geo-Spatial

AlertEnterprise!
AlertEnterprise Implementation

[SAP Applications]
1. SAP Financials
2. SAP Operations
3. SAP HCM
4. SAP SRM

[Physical Access and Surveillance]
1. Honeywell Pro-Watch
2. Lenel
3. Axis Communications

[Special Applications]
1. Treasury Manager
2. System Architect / Nucleus

[Non SAP and Legacy Applications]
1. PeopleSoft
2. AD
3. Computer Aided Dispatch

[Access to OSI & Process Systems]
1. OSI PI
2. AF
3. Outage Mgmt. System

[Utility EAM* and O&M* Application]
1. EAM – Enterprise Asset Management
2. O&M – Operations and Maintenance
3. SCADA – Supervisory Control And Data Acquisition
• Configurable RAS or Guided Procedures to avoid mistakes in panic

• Leverage existing Cameras, PACS system, Communication System for effective response

• Automated Remedial Actions – Inform First Responders, Lock the door, Trigger non-lethal weapon systems (like rubber bullets, sticky foam, non-lethal gas etc)
About AlertEnterprise

Flagship Customers
- Oklahoma Gas & Energy
- Allegheny Energy
- Nike
- The Coca Cola Company

Pilot Projects
- TSA – Top US Airports Security
- DHS, non-lethal weapon system

Experienced Team with Unparalleled Track Record
- Founded Application Security company Virsa Systems ($400M acquisition by SAP)

Most Innovative Company Awards
- RSA Security Conference ‘09
- Security Summit ‘09
- Demo Jam at SAP TechEd ‘08
- ASIS Top 10 Award ‘09

Key Partners
- SAP
- Oracle
- Cisco
- Lenel
- OSIsoft

Unfair Advantage
- Application Security Context & Domain Knowledge