Honeywell Security Group

Complying w/ NERC Physical Security Standards Webinar

NERC entities will soon have to comply with 3 physical security standards

Today's Host – Dave Karsch

Guest Speakers:
Donovan Tindill - Honeywell Process Solutions
Rob Saxton - First Energy

Call will start shortly!

Today's Speakers

Honeywell

Dave Karsch – *Today's Host*
Utility Market Lead
dave.karsch@honeywell.com
215-266-3473

Our guest speakers:

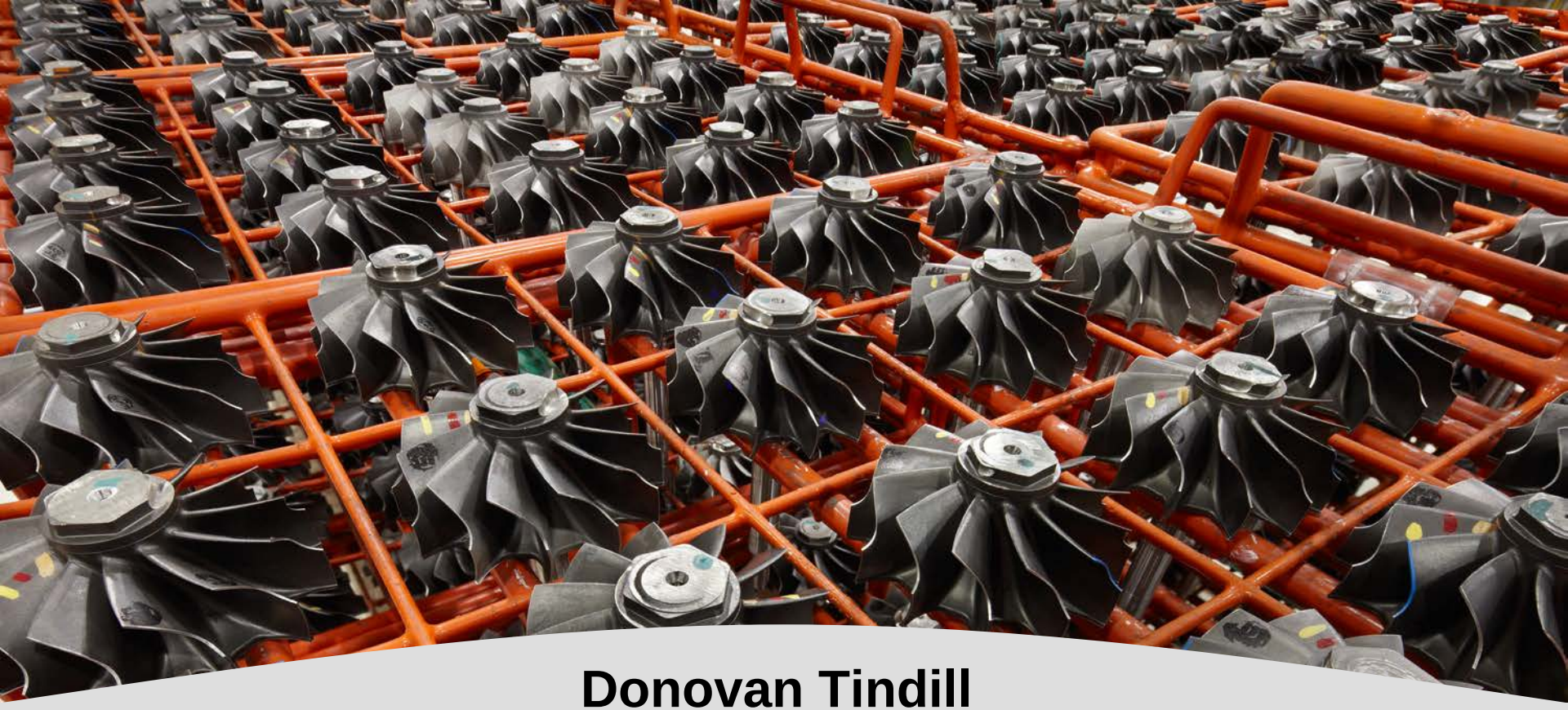
Rob Saxton
Security Technology Manager
First Energy Corporation

Donovan Tindill
Senior Security & Compliance Consultant
Honeywell Process Solutions

Additional Honeywell team on the call:
Deborah Paterson – HSG Marketing / Moderator

Today's Agenda

- What will new standards require for physical security controls?
- What will be the process and timeline be for complying with them?
- How is compliance with CIP-006 different in Version 5 vs. Version 3?
- Rob Saxton will discuss First Energy's plans to address the new regulations
- Invitation to participate in the Honeywell End Users Group / Utilities
- Honeywell Security Group – How our products and services will enable you to meet today's new regulations with our Integrated Solutions



Donovan Tindill
June 11, 2014

NERC Physical Security Regulations for the Power Industry

Honeywell

Physical Security

WHICH CIP STANDARDS?

The NERC Physical Security Landscape

Honeywell

- **Currently, NERC entities face just one set of physical security requirements: CIP-006 Version 3.**
  - Infamous “six-wall” perimeter.

- **In the next few years, there will be three physical security standards, all with different scope and objectives.**

Which Standards Cover Physical Security

Honeywell

- **CIP-006-3, currently in effect.**
- **New: CIP-014-1**
  - Fast-tracked standard to address immediate risk to critical transmission substations and control centers. Excludes generation.
- **New: CIP-003-6 R2.2**
  - Minimum requirements defined for Low Impact BES Cyber Systems.
- **New: ~~CIP-006-5~~, CIP-006-6**
  - For Medium and High impact BES Cyber Systems. Requires operational or procedural controls, one or more physical access controls, monitoring, alarming, incident response, logging, testing, and visitor control program.
  - CIP-006-6 adds encryption or physical protection of ESP network communications outside physical security perimeter.

Honeywell

CIP-014-1 for Substations and Control Centers
CIP-003-6 R2.2 for Low Impact
CIP-006-6 for Medium/High Impact

WHAT IS NEEDED TO COMPLY

CIP-014-1

Honeywell

- **Where did it come from?**
  - In early March, FERC ordered NERC to develop physical security requirements for critical substations and control centers and submit them for approval in 90 days.
  - Approved by NERC BoT in May, and now preparing the filing for FERC
- **Assuming FERC Q3 approval, it will go into effect on April 1, 2015.**

The Steps of CIP-014-1

Honeywell

1. **R1: Determine "critical" substations and the control center(s) that control them.**
   - Start with Medium impact substations as per CIP-002-5 Attachment 1, then evaluate those "critical" per CIP-014-1 R1. Must be verified by an unaffiliated third-party.
2. **R4: Conduct a physical vulnerability assessment of the "critical" substations and control centers.**
3. **R5: Develop *and implement* a plan for addressing the vulnerabilities identified in the second step.**
4. **R6: Have the vulnerability assessment and physical security plan verified by a third party.**

R1 initial assessment by effective date ~April 2015; balance required within the next ~180 calendar days.

- Date subject to change based on FERC approval.

Physical Security for “Lows”

Honeywell

- **In CIP Version 5, every facility that meets the new definition of the Bulk Electric System (BES) is at least Low impact.**
- **In general, the new BES definition refers to facilities that are connected at 100kV or higher, or blackstart facilities.**

- **Only CIP-003-5 R2 applied to Low impact requiring four policies (including a physical security policy). However, there was no content specified for those policies.**

Changes in CIP v5

Honeywell

- **FERC approved CIP Version 5 with conditions, including enhancement of requirements for Low impact.**
- **As CIP v5 is already approved, changes can only be made to the next version.**
  - V6 will include the four changes FERC ordered.
- **We expect to see CIP version 6 submitted to FERC by end of 2014, their possible approval in 2015, and v6 compliance date April 1, 2016.**
  - Low Impact has until April 1, 2017.

Physical Security in CIP v6

Honeywell

- **CIP-003-6 R2.2 reads (in the first draft): "Implement one or more documented processes that collectively address:**
  - 2.2.1 Operational or procedural control(s) to restrict physical access.
  - 2.2.2 Escorted access of visitors at Control Centers.
  - 2.2.3 Monitor physical access point(s) at Control Centers with external routable protocol paths."
- **2.2.1 is the only physical security requirement for transmission substations and generating stations.**
- **2.2.2 and 2.2.3 only apply to Low impact Control Centers.**

“Operational or Procedural Controls”

Honeywell

- An operational control might be a lock on the door, card reader, video surveillance, etc.
- A procedural control could be a guard with a sign-in book. Maybe just the sign-in book?
- It may be left to the discretion of the Responsible Entity, or FERC may require more detail. Too soon to tell how this will end up.
- We advise you to monitor what your NERC Regional Entity says about this – they are the final authority for your region.

Physical security for Mediums and Highs

Honeywell

- **CIP-006-5 prescribes physical security for Medium and High impact. V6 requires additional protection of communications cabling.**
  - Note: The “six-wall boundary” is no longer a requirement!
- **There are requirements for operational or procedural controls, one or more physical access controls, monitoring, alarming, incident response, logging, testing, and visitor control program.**
  - Many requirements only apply to High Impact BES Cyber Systems and Medium with External Routable Connectivity.
  - For Medium Impact BES Cyber Systems, external routable connectivity determines the applicable requirements.
- **Compliance is due April 1, 2016.**

Honeywell

CIP Physical Security Standards

WHEN TO COMPLY

When is Compliance Due?

Honeywell

- **CIP-014-1**
  - Critical Substations and their Control Centers: initial assessment by April 2015 and implement within 120-days (assuming Q3-2014 approval).
- **CIP-006-6**
  - High and Medium Impact: April 1, 2016 (assuming 2015 approval and no change to implementation plan).
- **CIP-003-6 R2.2**
  - Low Impact: Jan 1, 2018 (assuming 2015 approval and no change to implementation plan).

Honeywell Process Solutions

> Industrial IT Solutions

> Cyber Security & Compliance

WHERE TO GET HELP

Honeywell Industrial Cyber Security & Compliance

Honeywell

Industry Leading People and Experience

Global team of certified experts with deep experience across all industries
100's of successful PCN / Industrial cyber security projects
Leaders in security standards ISA99 / IEC62443 / NERC CIP

Industry Leading Processes and Expertise

Proprietary methodologies specific for process control environment & operations
Best practices developed through years of delivering solutions
Comprehensive understanding of unique process control security requirements

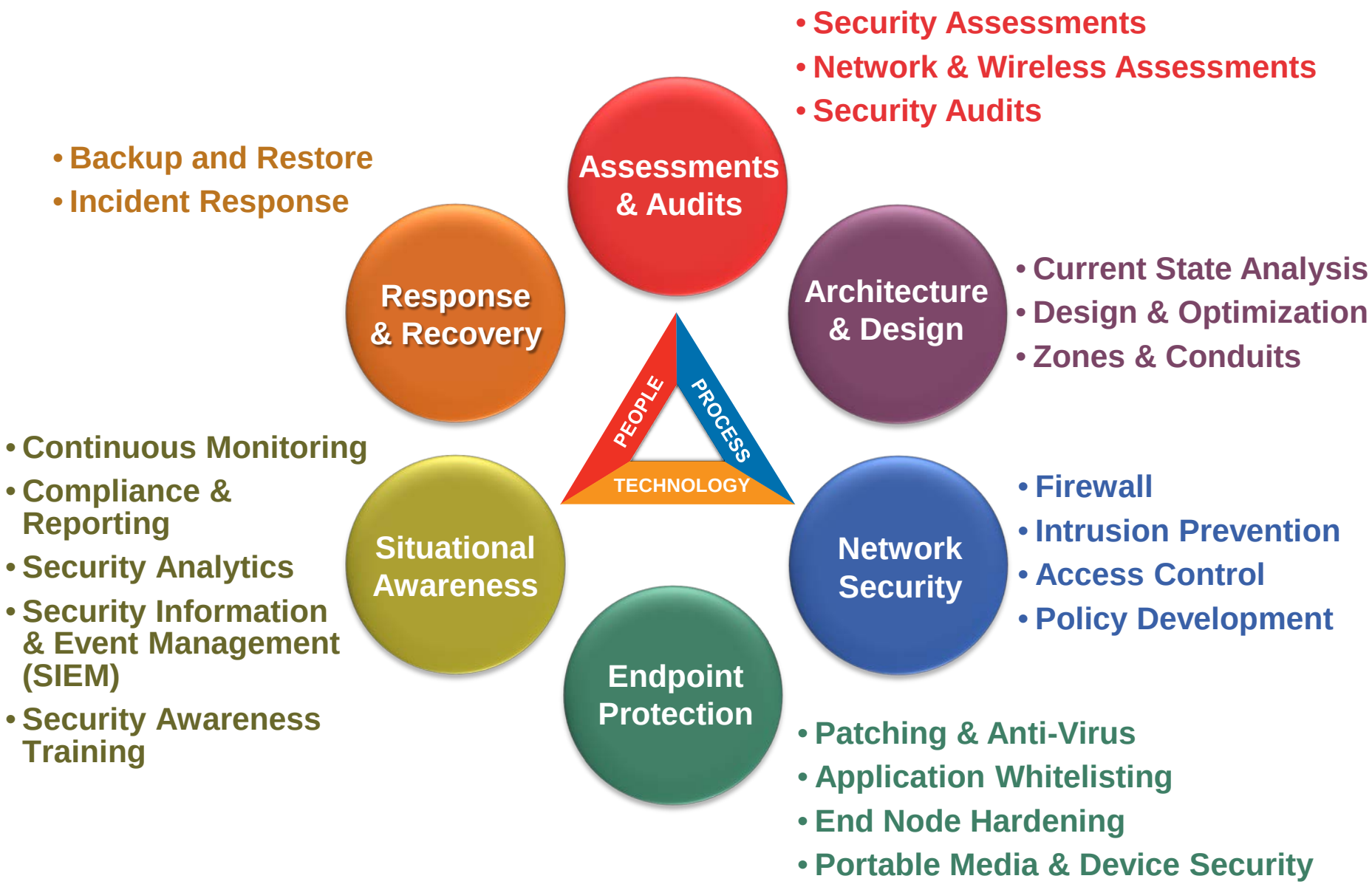
Industry Leading Technology

First to obtain ICS product security certification with ISASecure
Largest R&D investment in cyber security solutions and technology
Strategic partnerships with best in class security product vendors

Trusted, Proven Solution Provider

Complete Industrial Cyber Security Solutions

Honeywell



Honeywell Utility User Group

Regulatory Audit Success

Robert Saxton
FirstEnergy Corporate Security

FirstEnergy – Our Background

Honeywell

- **Facts at a Glance:**
  - Six million customers
  - More than 20,000 megawatts of generating capacity
  - Operations in six states
  - 65,000 square miles of service territory
  - 20,000 miles of high-voltage transmission lines
  - $47 billion in assets
  - $16 billion in annual revenues
  - 17,000 employees

FirstEnergy

FirstEnergy - Responsibilities

Honeywell

- **Corporate Security**
  - Regulatory Compliance
  - Business Continuity
  - Guard Services
  - Integrated Security Technology
  - IT Compliance
  - Cyber Security

FirstEnergy

FirstEnergy Compliance Program

Honeywell

- Critical Assets:109
- CCAs: 646
- EACM: 145
- NCCA: 650
- PACS: 78

FirstEnergy

FirstEnergy System Overview

Honeywell

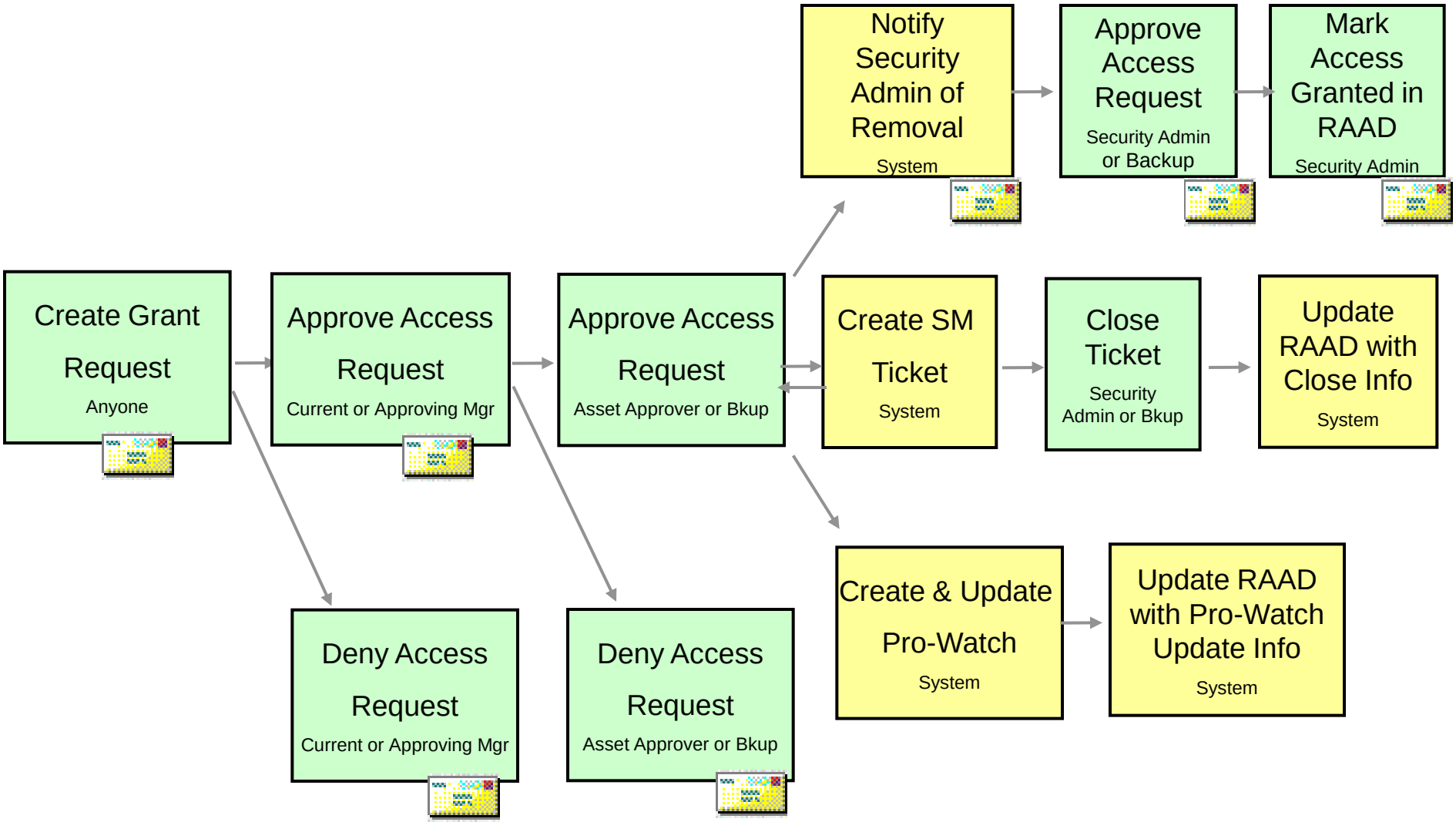
- Readers: 2600+
- Badge Holders: 27,500
- Sites today: 285
- Camera’s Today: 3000

- **CipV5 Planning**
  - Team established to determine business needs.
  - Definitions established for business to identify BES system
  - Concerns at this point of timeline and scope, Low Impact ruling, 24 hr removal
  - Working with Honeywell on new requirements such as limiting / notification of login attempts of panels
  - Importance of peer reviews and industry standards
    - NATF, HIS, Etc

- **2012 NERC Audit Key Program Features Highlighted**
  - RAAD (Regulated Access Authorization Database)
  - Compliance Reporting Tool
  - Electronic Registration of Remote Visitors
  - Remote Clients
    - Clients access through terminal servers
    - Multiple authentication
  - PW 6000 panels
    - One Firmware
    - Removal of User/ Password

Regulatory Access Authorization Database - Grant

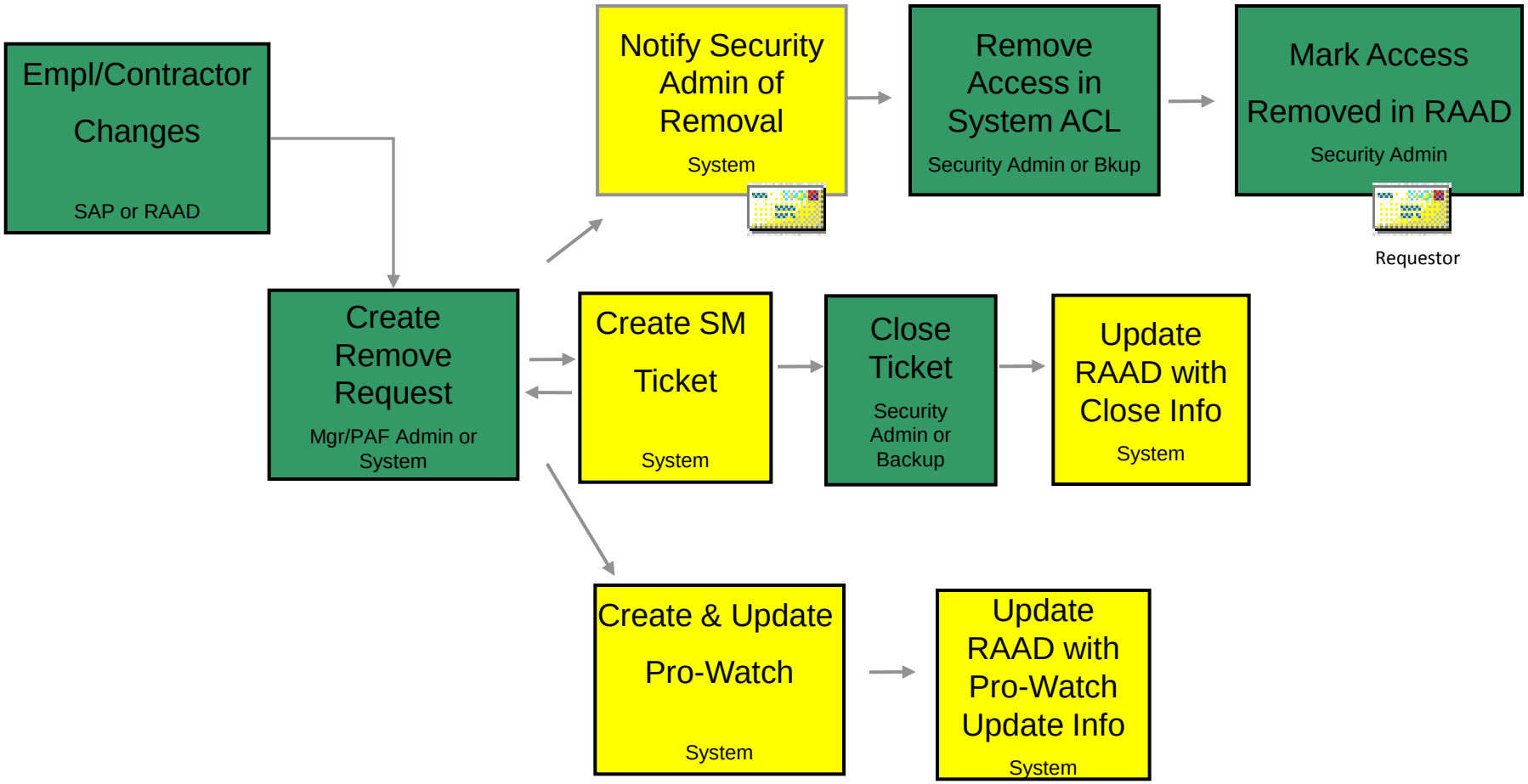
Honeywell



FirstEnergy

Regulatory Access Authorization Database – Removal

Honeywell



FirstEnergy

Pro-Watch End-User Forum – Utility Vertical

Honeywell

Join the Honeywell End Users Utilities Group
Rob Saxton – Chairmen Utility Vertical
Annual Meeting in 2015 in TN
Group calls to discuss Utility specific issues

Honeywell Security Group Overview

Honeywell

- **Pro-Watch® is our enterprise access control product (PACS) that is very modular – open and scalable to integrate with our family of solutions.**
- **Honeywell (HSG) sells over $2.8 billion of security products annually.**
- **Honeywell manufactures access, intrusion, video and Vindicator products all to integrate seamlessly!**
- **Honeywell (HSG) has factory direct representatives to help you solve your strategic business problems and trained authorized integrators to support your projects.**

Physical Security - Pro-Watch Ecosystem

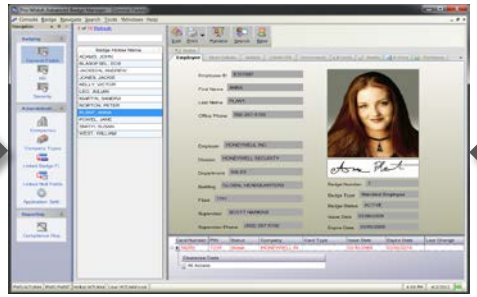
Honeywell

Integrated Solution Topology

Honeywell

User Interface

Vindicator® Intruder



Pro-Watch® Access

MAXPRO® VMS Video

Network

Record and Control hardware

Intruder Controllers

V3 & V5 Vindicator Controllers

Access Controllers

Honeywell, Mercury, Casi-Rusco Controllers
Smart Locks

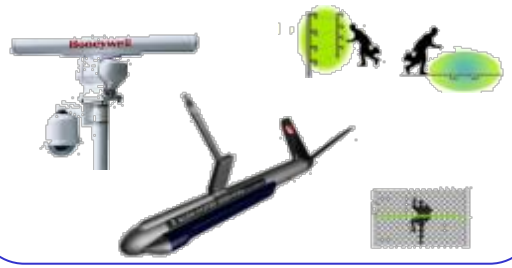
Recorders

MAXPRO NVR & Hybrid Recorder

3rd party recorders

Field Sensors and devices

Perimeter Sensors



Readers, Locks Gates, Turnstiles

Industry standard locks, ASSA, Salto …

Cameras

Honeywell, 3rd party, ONVIF & PSIA

ONVIF

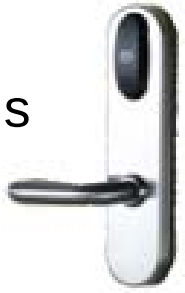
Pro-Watch Continued Ecosystem Development

Honeywell

Jun 2013

- **Pro-Watch 4.1**
  - Vindicator Integration
  - Salto Disconnected Locks
  - Native Integration of Mercury's Equivalent Honeywell Panels
    - PW3000, PW5000, PW6000 & PW6101
  - Integration Kit Enhancements
  - Strong Field Sensor Integration like Radar

Vindicator **Pro-Watch** **MAXPRO**



Feb 2014

- **Pro-Watch 4.1 SP2**
  - Support for Mercury's M5 Series board CASI-Rusco Micro5 replacement.
  - Pro-Watch continues to be a Leader in Open Scalable Platforms

Pro-Watch Ecosystem Development

Honeywell

July 2014

- Pro-Watch 4.2
  - Salto Sallis Wireless Locks
  - Assa Abloy Aperio Wireless Locks
  - Morpho Biometric Readers
  - Support for Microsoft SQL Server 2012
  - Support for Windows Server 2012/2012 R2
  - Support for Windows 8/8.1

Microsoft SQL Server 2012

Windows Server 2012

About Substation Security….

Honeywell

- We all understand the attacks that caused concern and regulations to protect our BES.
- FERC issued new guidelines for protecting substations.
- We will be glad to discuss this with you…
- Remember it is better to involve the third party to verify your critical substations from the start of the process vs. just at the end.
- Design a sustainable “early warning” system that can reduce the site risk to compromise.

Securing your Medium Assets

Honeywell

- Monitor for unauthorized access / *Pro-Watch PACS*
- Alarm / alert within 15 minutes of unauthorized access
- Monitor / alert for Physical Access Control Systems (PACS) – *Using our MAXPRO PE Recorder with Analytics*
- Log initial entry *and* exit
- Continuously escort visitors without unescorted access privileges –*Visitor Management – LobbyWorks®*
- Maintain and test systems every 24 months. *Honeywell Professional Services and System Optimizations*

True Open Platform - Pro-Watch®

Honeywell

- Open, modular, scalable, & sustainable to meet stringent regulations.
- Third-party systems integration—resulting in cost savings and increased operational efficiencies.
- Seamless integration with Vindicator's high security intrusion detection for hardened perimeters.
- Integrates seamlessly to visitor management, mass notification and other systems for tighter security
- Ease and proven integration to HR systems such as SAP, this is critical for terminations processing. High end integrations to Alert Enterprise.
- Ease of recovery backup sites to align with primary sites and where data centers fall

Pro-Watch® – Features to meet NERC CIP requirements

Honeywell

- **NERC CIP Key Program Features Highlighted**
  - Direct integration to your Regulated Access Authorization Database
  - Pro-Watch Compliance Reporting Tool
  - Pro-Watch's Electronic Registration of Remote Visitors
  - Our Regular Publications on Ports Required and Patch Testing
  - Remote Clients
    - Clients access through terminal servers
    - Multiple authentication
  - Pro-Watch Field Hardware - PW 6000 panels
    - One Firmware
    - Removal of User/ Password
    - Support of open port management

We Publish – Required Ports and Monthly Testing

Honeywell

- **The following information is provided in response to requests on CIP information**:
- R2 Ports & Services **Pro-Watch®** Port Settings
- **Pro-Watch®** Server requires ports *** (for named pipes)
- **Pro-Watch®** uses port *** (for badging file sharing)
- **Pro-Watch®** also uses port *** (to communicate to SQL)
- If the **Pro-Watch®** system has panels on the network, we typically use port *** but they can use any port for panel communications.
- **Pro-Watch®** PW-6000 Port Settings UDP Port **/** can't be disabled on the controller.
- They are used to handle DHCP when connecting the controller to IP enabled reader boards.
- UDP Port *** can be disabled by turning off Zeroconf/Bonjour on the controller.
- Information on the ports kept up to date

May 31, 2014

Your Organization.
123 Power Way
Anywhere, US 1976

ProWatch customers monthly updates,

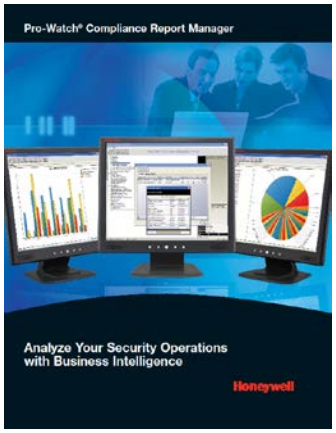
- **Security & Malware patches are neither technically feasible nor necessary for Honeywell Security's Access Control hardware products.**
- **The current version of PW6K1IC firmware for Pro-Watch releases prior to PW 4.1 SP2 is 2.054. The latest firmware for PW6K1IC for Pro-Watch release PW4.1 SP2 is 2.062. The latest firmware version for PW5K1IC and PW3K1IC is 2.092. The latest firmware version for PW6101ICE is 1.176. Firmware files are available on the ftp site.**
- **Pro-Watch 4.1 SP 2 was officially released in February 21, 2014. Release notes have been posted to www.honeywellintegrated.com.**
- **Let me know if you would like PW 4.1 SP2 software for your test environment.**
- **The link below provides a history of all approved Microsoft patches.**
- **https://www.honeywellintegrated.com/documents/7_201027_03_MSpatch.pdf**
- **We have not released any Pro-Watch security patches.**

Regards,
Dave Karsch
Utility Lead – Regulated Markets
215-266-3473

Integrated Compliance Reporting & Visitor Management

Honeywell

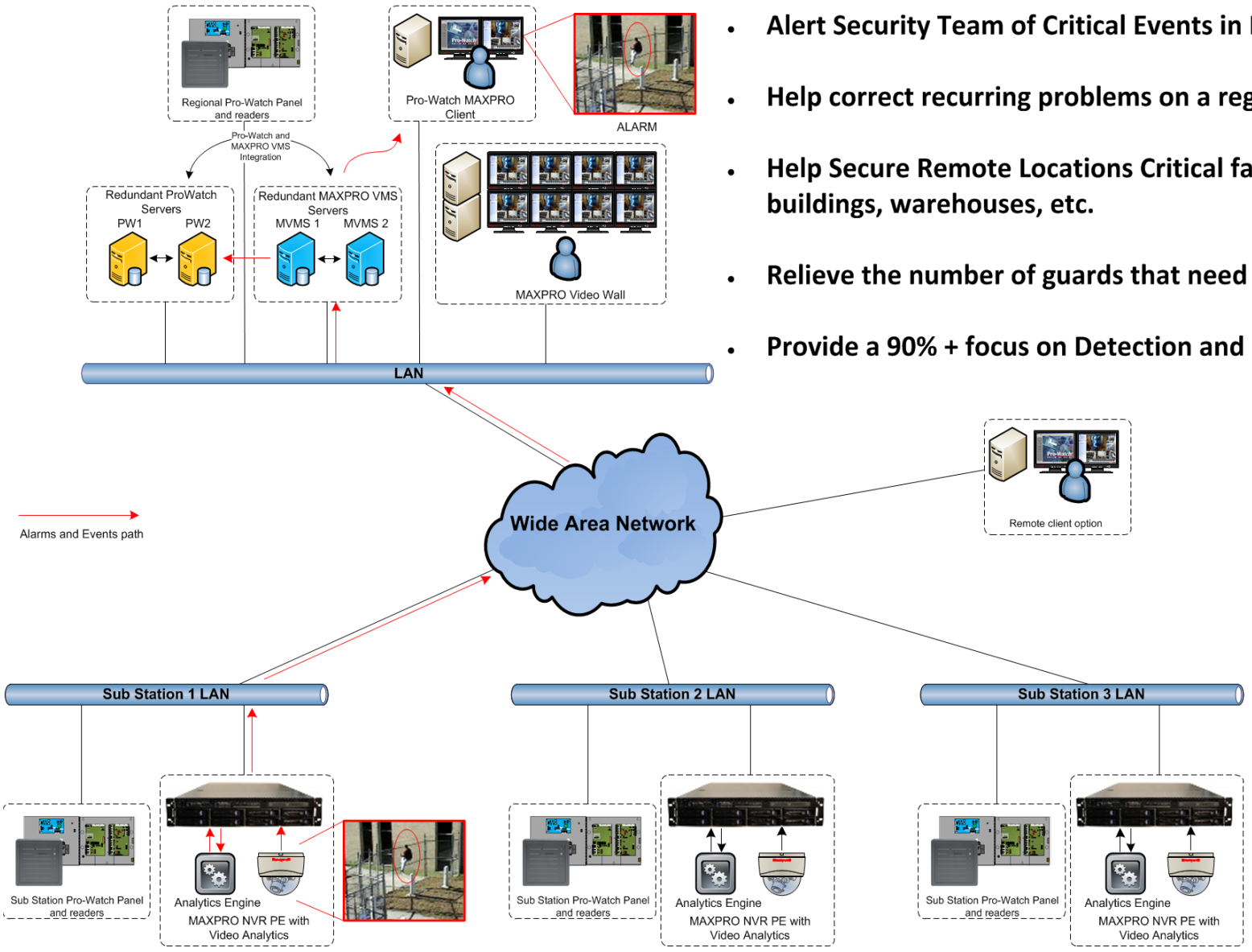
- **Standardized Reporting**
  - Standard format for CIP alarm response
  - Quarterly Reviews
    - Automated Report Generated for all Physical Assets
  - Easy identification of any discrepancies
  - Pro-Watch Compliance Reports



- **LobbyWorks®**
  - Tracking and reporting of regulated sites
  - Standardized reports/ logging
  - Required fields ensures capture of all required information
  - Integrated with Pro-Watch and our Compliance Reports tool

What MAXPRO NVR Analytics & MAXPRO VMS do for you?

Honeywell



- **Alert Security Team of Critical Events in Real Time**
- **Help correct recurring problems on a regular basis**
- **Help Secure Remote Locations Critical facilities, corporate buildings, warehouses, etc.**
- **Relieve the number of guards that need to be posted**
- **Provide a 90% + focus on Detection and Intrusion**

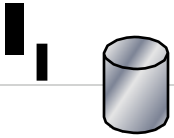
Pro-Watch /Vindicator Integration

Honeywell

Requirements:

- Pro-Watch 4.1 or newer
- Vindicator Application Module
- HSDK 2.0 (License ONLY)
- Vindicator V3 IDS
  - PC Smart Pak Config Tool
  - *Optional*: UHS-1500 Field Panel
- *Optional*: Vindicator Command and Control 2 (VCC2)

Pro-Watch Server
HSDK Enabled
Vindicator App Module



Pro-Watch
SQL DB

Vindicator Pro- Watch
App Module
Configuration GUI

Vindicator V3 IDS

UHS-1500
(optional)

VCC2
(optional)

- Additional Information
  - Intrusion alarm point configuration is done on V3 via PC Smart Pak
  - Pro-Watch Server, Vindicator Application Module and VCC2 can co-exist on one server

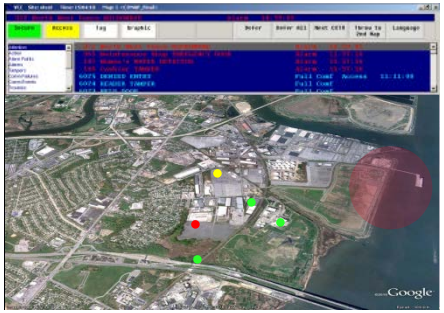
Use Case Example

Honeywell

.**Security Issues and Challenges**:

- Vandalism, eco terrorism, disgruntled employees and/or citizens
- NERC/CIP regulations and requirements Low-Med-High
- Site unmanned at times

- **Existing Conditions**:
  - Chain link fence around perimeter and metal buildings



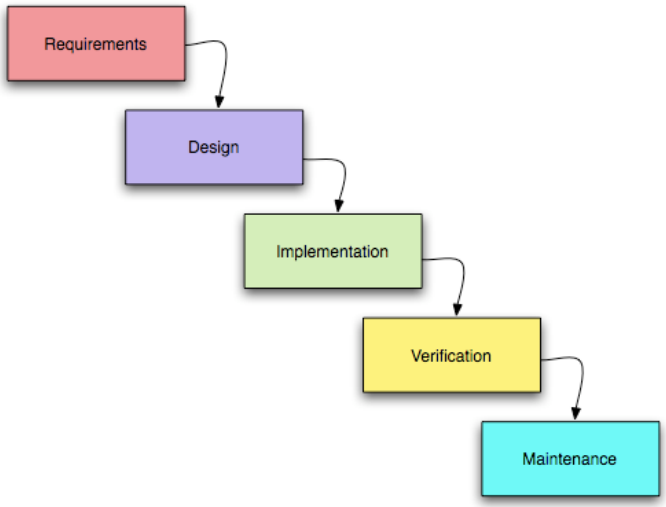
- **Honeywell Solution (100% out-of-the-box integration)**
  - Access control and overall security mgmt (Pro-Watch)
  - Assessment (MAXPRO VMS)
    - Monitors perimeter, all critical in-plant equipment and interior areas
    - Video analytics along fence line
  - Perimeter and interior intrusion (Vindicator)
    - Live graphical map display of entire facility
    - Optional - Ground based radars for perimeter and UAV monitoring (targets auto-tracked via cameras)
    - Interior IDS
- **Value**
  - Reduced liability and meeting regulatory requirements of NERC/CIP

Migration Process to Pro-Watch

Honeywell

Project planning and design phase:

- Define the scope-of-work using proven migration best-practices
- Identify migration sites and existing hardware count
- Develop a cost/benefit analysis using Honeywell Pro-Watch spreadsheet
- Assign optional Honeywell resource and project manager working with stakeholder



Advantages of Pro-Watch®

Honeywell

- Web-based Reporting
- Open Hardware Platform
- Support for non-Honeywell branded Mercury and Casi Micro5 Line based panels
- Pro-Watch PSIM like Physical Access Control Product
- Supports Video Analytics and Radar for Substations
- Pro-Watch has Partner support all over North America
- Open – Scalable – Modular – Sustainable Integration

Questions?

Honeywell

- Please send comments or suggestions to Dave Karsch, I will coordinate questions with our team for answers and follow-up.

- Consider attending our next educational webinar in October.

- Should we add additional people to our next webinar? If yes, send contact information to dave.karsch@honeywell.com or donovan.tindill@honeywell.com

Thank you for participating in today's call!