Cyber Security & Instrumentation and Controls

Bill May

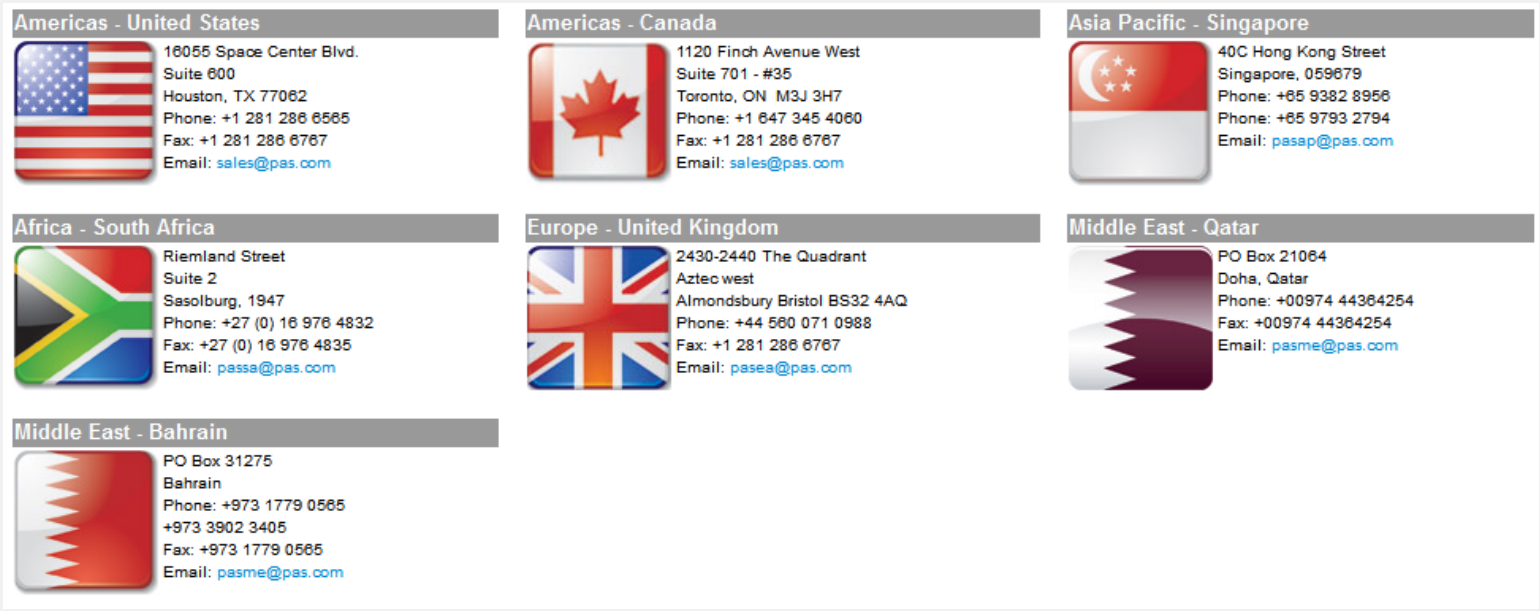
Executive, Global Strategic Projects

PAS, Inc.

Houston, TX

Introductions

- PAS, Inc.
  - Founded in 1993 as Plant Automation Services
  - Global Provider of software solutions
    - Large install base, across multiple industries
  - Operations Effectiveness
  - Automation Asset Management
  - Regional Offices:



Americas - United States

16055 Space Center Blvd.
Suite 600
Houston, TX 77062
Phone: +1 281 286 6565
Fax: +1 281 286 6767
Email: sales@pas.com

Americas - Canada

1120 Finch Avenue West
Suite 701 - #35
Toronto, ON M3J 3H7
Phone: +1 647 345 4060
Fax: +1 281 286 6767
Email: sales@pas.com

Asia Pacific - Singapore

40C Hong Kong Street
Singapore, 059679
Phone: +65 9382 8956
Phone: +65 9793 2794
Email: pasap@pas.com

Africa - South Africa

Riemland Street
Suite 2
Sasolburg, 1947
Phone: +27 (0) 16 976 4832
Fax: +27 (0) 16 976 4835
Email: passa@pas.com

Europe - United Kingdom

2430-2440 The Quadrant
Aztec west
Almondsbury Bristol BS32 4AQ
Phone: +44 560 071 0988
Fax: +1 281 286 6767
Email: pasea@pas.com

Middle East - Qatar

PO Box 21064
Doha, Qatar
Phone: +00974 44364254
Fax: +00974 44364254
Email: pasme@pas.com

Middle East - Bahrain

PO Box 31275
Bahrain
Phone: +973 1779 0565
+973 3902 3405
Fax: +973 1779 0565
Email: pasme@pas.com

Definitions

- Configuration
- Cyber Security
- Cyber Automation Assets
- Cyber Attacks:
  - Espionage, Warfare, Crime, Vandalism, “Hactivism”, Sabotage, etc.
- Management of Change
- NERC CIP
- **Saboteurs**

  “...derives from the Netherlands in the 15th century when workers would throw their sabots (wooden shoes) into the wooden gears of the textile looms to break the cogs, fearing the automated machines would render the human workers obsolete.” - *wikipedia*

Software Solution

- PAS Objectives for I&C Cyber Security
  - Ensure system reliability through increased cyber-security solutions specifically designed for control system environments
  - Increase efficiencies by providing software solutions to automate repetitive compliance tasks
  - Provide change tracking history for audits
  - Provide a Management of Change solution that includes, “ex post facto” MOC combined with data validation

The Challenge of Compliance & Security

- Understanding current compliance/regulations is difficult
  - Multiple sources of information, multiple ways to be in violation, ever changing list of compliance items
- Cyber-Security Deployment and Maintenance is challenging
  - IT Networks/Automation Networks Various layers/levels of assets
    - Multiple vendors, versions, locations
    - Many systems are “quasi-connected”
    - User Access to systems are difficult to manage
    - Non-standard approach to systems management
- In addition specific requirements are resource intensive
  - Extremely time consuming
  - Prone to error through data omission
  - Manual data collection must be repeated
  - Effort to reach compliance measured in months

Recent Violation

- April 2012 - $115K fine for NERC CIP violations
  - One cited violation, failure to document / implement anti-virus software

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity (URE), NERC Registry ID# NCRXXXXX, in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

URE submitted to Reliability*First* Corporation (Reliability*First*) self reports of possible violations of nine CIP Standards listed as follows: CIP-007-1 R3, CIP-007-3 R4.1, CIP-007-3 R6, CIP-004-2 R4.2, CIP-002-3 R3, CIP-006-3 R1, CIP-007-3 R1, CIP-007-3 R2, and CIP-007-3 R6.

CIP-007-3 R4.1 provides in pertinent part:

R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

http://www.nerc.com/filez/enforcement/Public_FinalFiled_NOP_NOC-971.pdf

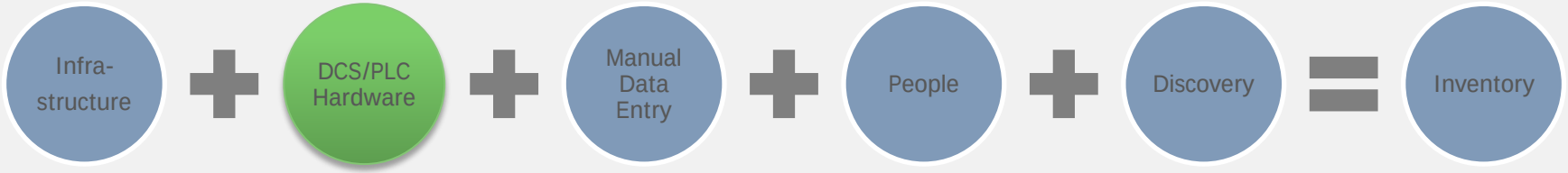
CIP Inventory

- What is an Asset Inventory?

CIP Inventory

- Ports
- Services
- Patches
- Applications
- Events
- Other Stuff (OS,etc.)

CIP Inventory



- Application Work Stations
- Operator Work Stations
- Engineering Work Stations
- I/O Cards/FBMs
- Controllers

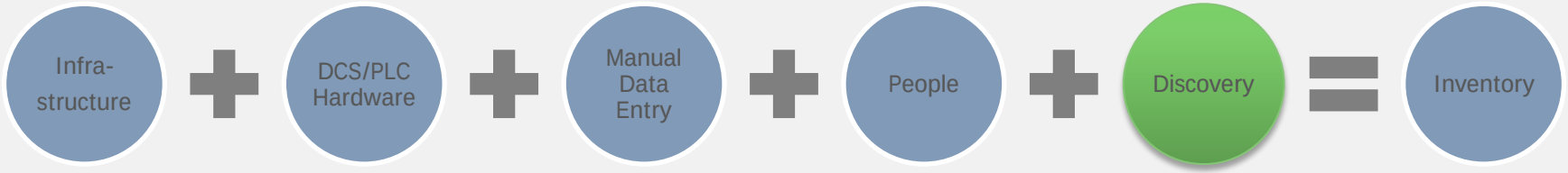
CIP Inventory

- Plant Criticality
- Black Start
- Must Run
- Megawatts
- Routable Protocol
- Modem Connection
- Cyber Critical Asset
- Reference ID
- ESP Segment ID
- External Accessibility ID
- PSP Boundary ID
- Appropriate Use Banner

CIP Inventory

- Users
- Access
- Passwords
- Training
- More…

CIP Inventory



- Approved Devices
- Unapproved Devices

CIP Inventory

The sum of the parts = 1 inventory item

Challenges / Solutions

- **Asset Inventory**
  - Complete asset inventory, in a standard hierarchy, updated on a regularly scheduled basis
- **Change Control & Configuration Management**
  - Tracking all modifications to Critical Cyber Assets, (hardware or software), automatically when possible, & MOC
- **Ports, Services, & Programs**
  - Tracking ports and services to ensure settings remain compliant. Anything not approved as part of COE will be identified and reported
- **Patch Inventory and Management**
  - The ability to visualize where patches are required, when patches have been deployed, which assets are not current on patches and require TSE's

Benefits

- Resourcing for asset inventories can be greatly reduced
- Automated inventories provide reports quickly
- More frequent assessments
- Defects are found more easily
- Broader Awareness Increases Intrusion Detection
- Violations are reduced
- Accuracy is increased

Project Case –Power Generator, multiple site implementation

- Required Resources: Reduced by a factor of four
- Inventory Task Duration: Reduced by a factor of six
- Automatic generation of compliance reports and dashboards

Thank You

Contact Information:

Bill May

Direct: 281-709-0127

Office: 281-286-6565 x146

email: bmay@pas.com

web: www.pas.com