ICS Cybersecurity. Safety. Compliance.

PAS Cybersecurity
Services Proposal for City of Aurora

PREPARED FOR
Mr. Ted Beck
City of Aurora
Email:
Tbeck@aurora-il.org

PREPARED BY
Michael Montanus

16055 Space Center Blvd, Suite 600
Houston, TX 77062
Ph.: 832-985-4092
Fax: 1-832-645-7686
Email: mmontanus@pas.com

PROPOSAL DATE
May 10, 2018

PROPOSAL
PL71114

Version Table

Version	Summary	Date
V.1	Initial Issuance	January 2, 2018
V.2	Mark up clarifications via WPD dated Jan 22, 2018	February 14, 2018
V.3	Revisions based on latest WPD feedback	March 27, 2018
V.4	Changed from daily rate to hourly rate. Not to Exceed added in.	April 15, 2018
V.5	Added in project schedule	April 16, 2018
V.6	Inserted payment terms	May 5, 2018
V.7	Reduced time by 8 hours based on June 12 PO commitment	May 10, 2018

Table of Contents

1 Executive Summary

PAS is pleased to submit this proposal in response to the City of Aurora's expression of interest to undertake a current-state industrial automation control system (IACS) security assessment. This proposal details PAS' proposed methodology, schedule, budgetary requirements and capability to undertake this assessment.

PAS understands the City of Aurora (CoA) has several critical Operational Technology (OT) and Industrial Automation Control Systems (IACS) assets. A cybersecurity incident on these control system assets, whether is it intentional or unintentional, may disrupt essential services with potential for significant consequences to the city and its customers.

PAS supports CoA's objective to be proactive and review the scope of assets to gain an understanding of the IACS Cybersecurity vulnerabilities, security strengths, weaknesses and risks.

PAS' approach in achieving CoA's goals will be based on proven methodologies as detailed in Section 2 of this proposal. This will enable CoA to understand where vulnerabilities exist within their current environment, what actions are required to strengthen the organization's IACS security posture against new and future emerging cyber threats and allow the reduction of risk to acceptable levels. PAS is confident that our solution and services offered will meet and exceed CoA's stated objectives and are looking forward to the potential of teaming with CoA on this critical project.

Best Regards,

Michael Montanus

Cyber Account Manager| PAS Global, LLC
Phone: 832-985-4092 Email: MMontanus@pas.com

2 Scope of Work

2.1 Statement of Work

PAS is pleased to provide network consulting services to evaluate the current network design and analyze the current security in-place for the PCN at CoA. A report outlining recommendations based on PAS best practices recommendations will be provided.

In order to effectively assess the PCN, it will be necessary to conduct an on-site evaluation to gain insight into the existing infrastructure. The on-site work will be done by PAS consultants and will be approximately one week in duration. The report will be issued in approximately three weeks after the completion of the on-site activity. PAS's approach to achieving CoA's goals will be based on proven methodology using PAS consultants deep IACS Cybersecurity experience. The below figure provides an overview of the key work activities and inputs performed as part of PAS' methodology for this engagement.

PAS has a clear understanding of CoA's objectives for this assessment. To achieve these PAS proposes the following phases, tasks and activities:

2.1.1 IACS Cybersecurity Assessment – Phase 1 - Planning

In this phase the following activities would be performed:

- IACS Cybersecurity assessment kickoff meeting with CoA's key stakeholders which will outline the following:
    - The CoA security assessment scope
    - PAS Team
    - Plan / Schedule of activities
    - Locations
    - Security framework methodology

Deliverables

- Kick-off presentation
- Project schedule & plan
- Site contact names, e-mail addresses and contact numbers.
- Coordinate interview schedules for all pertinent customer contacts.

Requirements

- CoA Facilities (Conference room and high-resolution projector or TV)

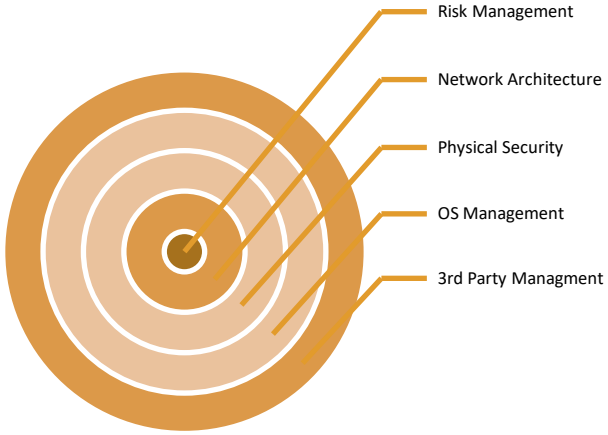
2.1.2 ICS Cybersecurity Assessment – Phase 2 – Assessments

Staff involvement
PAS suggest the following types of roles are interviewed during this stage:

- CoA Chief Information Security Officer (CISO)
- CoA Facility/Automation Manager – (3rd Party)
- CoA Network Manager
- CoA Automation Lead – (3rd Party)

Most interviews will require approximately 30 minutes with the site staff (listed above) requiring slightly longer time. These interviews can be performed remotely and/or on-site.

Scope
Without an effective cyber security regimen, the fundamental mission of process control, to ensure safe and reliable operations, can be compromised by an ordinary cyber threat such as a virus or worm. Therefore, a comprehensive cyber security strategy that employs a defense in depth model must be an essential element of every process control and safety system implementation.



In this diagram, Defense-In-Depth strategy elements for securing the process control environment is pictured

PAS recommends a defense in depth approach for protecting a facility's physical and cyber security. This includes an open source assessment, external vulnerability scanning and the on-site activity.

- PAS will conduct an external vulnerability assessment of CoA's ICS assets which will consist of the following:
    - Open Source Intelligence (OSINT) gathering to identify potential CoA targets above what is provided by CoA.
    - External vulnerability evaluation of CoA's Internet facing ICS Operating systems and applications.

The onsite activity will include evaluating the cyber security controls related to the people, processes and technology present at CoA. In this phase the following evaluations will be performed:

- Regular risk and vulnerability assessments
- Tiered networks with cyber security access restrictions at each level
- Hardened configurations deployed on PCs and servers
- Properly segmented process control and enterprise networks with limited access points
- Patch management and Anti-virus deployment strategies
- Management of Change
- Supply Chain Management
- Disaster recovery and Business continuity
- Best practices, policies and procedures

PAS will effectively assess the control network by steering the following onsite activities:

- Interviewing key personnel
- Analyzing Microsoft Patch Levels on all nodes
- Performing a basic walk through of critical areas of the Plant (PCN) components
- Surveying the existing perimeter
- Reviewing Switches/routers/firewall configurations
- DMZ (Demilitarized Zone)
- IDS (Intrusion Detection System)
- Reviewing password security on servers/workstations and infrastructure equipment
- Gathering network device information
- Reviewing current security policies and procedures
- Active Directory review
- Identifying the level of alerting and logging being performed
- Reviewing 3rd party interfaces

The collected data will be analyzed, and recommendations provided based upon the findings in the areas listed in this scope of work. PAS's recommendations will include improvements, additions, changes, and associated security improvements for the network(s).

PAS will provide an on-site analysis of the current cyber security processes, procedures, and safeguards used to protect the Process Control Network (PCN) from external threats. The analysis will then be used to create a Security Assessment Report that outlines observations, best practices, and site-specific recommendations to assist our customer mitigate any identified threats and/or vulnerabilities.

Deliverables

- Customer will be required to provide the following:
    - Current necessary as-built diagrams reflecting network architecture.
    - Configuration data for firewalls, routers, and switches
    - Internet facing nodes to be scanned (IP Addresses)
    - Process Application's communication requirements
    - Future expansion plans
    - Security policies and procedures
    - Known security issues or breeches
    - Specific issues to be addressed during assessment
    - Fiber path/layout drawings with distance

2.1.3 ICS Cybersecurity Assessment – Phase 3 – Reporting

In this phase the output of the interviews, risk assessments, documentation, and control testing results would be compiled into a report for CoA which would include:

- Executive summary
    - Summary of risks
    - Summary of recommendations
- Security maturity evaluation
- Risk & Vulnerability details

Deliverables

- Open Source Intelligence Report
- External Vulnerability Evaluation Report
- Draft ICS Cybersecurity Assessment Report
- Draft Maturity Assessment Report
- Final ICS Cybersecurity Assessment Report (including Maturity report)
    - Presentation of findings, conclusions and recommendations
- Workshop

Requirements

- PAS will present the final documents to CoA. This presentation is typically done remotely.
- PAS will facilitate a risk workshop with CoA's key stakeholders to document key business objectives, risk tolerance, internal/external risks, and risk impact(s) to the organization such as:
    - Financial risks
    - Operational risks
    - Marketplace risks
    - Brand/reputation risk
    - Compliance risks
- The timeline of the risk workshop will be coordinated with CoA.

2.2 Project Management

The PAS Project Management process is a stepwise methodology for project execution. It brings together the concepts, methods, and practices that have proven to deliver maximum return on investments.

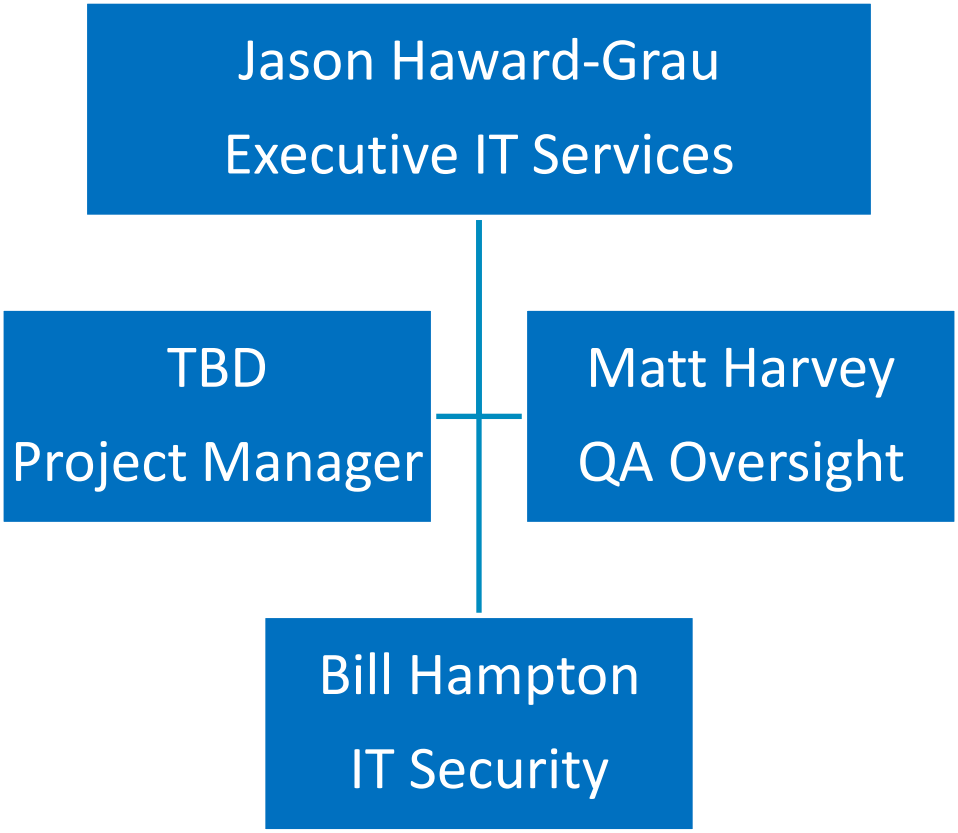
Customer Requirements

- Availability and access to site personnel for project execution
- Understand PAS project management and project change management practices to be outlined during the project kick-off meeting
- Timely responses for document review and approvals (Timely within 1 week)

Deliverables

- Project kick-off meeting
- Project status updates
- Project schedule management
- Project specific documents
- Project financials

2.3 Consultant Team



2.3.1 Consulting Lead

Name: Bill O. Hampton
Title: Cyber Security Consultant

Certifications:

- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- Certified Cisco Network Administrator (CCNA)
- GIAC Security Essentials Certified (GSEC)

Relevant Experience:
Bill has over 17 years of experience in Security, Compliance, Audit, Infrastructure, IT Operations, Project Management & Product Development Lifecycle Management with "traditional" information systems as well as Industrial Automation and Control Systems (IACS) over a variety of industries including the Energy sector. Bill has extensive experience in designing secure networks as well as conducting audits, risk, and vulnerability assessments.

2.3.2 QA Oversight

Name: Matt Harvey
Title: ICS Cyber Security Consultant

Certifications:

- Global Industrial Cyber Security Professional (GICSP)
- Certified Information Security Manager (CISM)
- SABSA Chartered Foundation Certificate – IT Security Architecture
- PRINCE2 Practitioner

Relevant Experience:
Matt Harvey is an experienced and competent Industrial Control Systems (ICS) professional with a career spanning over 20 years', from installing and maintaining instruments and controllers in the field, to conducting process control improvement projects using PRINCE2 and Six Sigma methodologies and then managing technical support teams. He has over 8 years' recent experience in ICS Cybersecurity leading teams directly from within operations and as a consultant completing assessments and developing strategies as well as holistic security architectures.

2.4 Preliminary Project Schedule

CoA Assessment High Level Schedule			
Activity	**Sub-Task**	**Start**	**Duration (Hours)**
Planning		Week 1	**8**
	Kick-off Meeting		4
	Confirm Schedule		4
	CoA to provide:		
	System Architecture, Site Access Requirements, Target external facing domain information.		
Assessment		Week 2	**64**
	Open Source Assessment		12
	PAS to gather information about the organization:		
	Conducting search queries across dozens of resources; Access restricted information through cached results; Conduct thorough searches on all social networks Search geo-location data within Twitter, and Instagram streams; Retrieve subscriber information from any landline or cellular telephone number; Search historical deleted versions of websites; View multiple historic satellite images and street views of any location; Identify all social networks in use by target domain;		
	External Vulnerabilty Assessment		12
	The following steps were part of this assessment:		
	Catalog assets and resources in a system; Identify the security vulnerabilities or potential threats to each resource; Provide a description of the vulnerability; Provide a risk factor for the associated vulnerability;		
	Onsite CS Assessment (Including 2 Travel Days)		40
	The following activities will be performed:		
	Travel Day - Monday		
	Conduct site visits to interview staff; Review system and security architecture; Perform walk-throughs with CoA control owners; Run network discovery scan; Run Windows system utility tool on a sample of systems; Gather network device configurations (FW's, Routers, Switches)		
	Travel Day - Friday		
Reporting		Week 3	**108**
	Data Analysis		20
	Develop Open Intelligence Source Assessment Report		12
	Develop External Vulnerability Report		12
	Develop CS Assessment Report		32
	Develop C2M2 Assessment Report		32
	Deliver (draft) reports		0
Follow-Up			8
	Final Deliverables & Executive Briefing		**8**
Total Hours			**188**

Work Onsite
Work From PAS

3 Commercial

3.1 Cybersecurity Services

Cybersecurity Consulting Services

- ICS cybersecurity assessment of CoA sites
  - City of Aurora Location
- Final Assessment Report to include the current processes and recommendations:
  - Effectiveness of risk management and assessment processes
  - Firewall Review
  - Network Design
  - Effectiveness of Patching Process and Procedures
  - Effectiveness of Inventory Management and Control
  - Effectiveness of Configuration Change Management
  - Effectiveness of Account and Access Controls
  - Effectiveness of Incident Response
  - Assessment of Business Continuity
  - Data Sharing (data feeds from ICS networks)
  - Effectiveness of Remote Access Controls
  - Password Management
  - Supplier Security Management
  - Security Controls
    - Physical
    - Network
  - Recommendations for monitoring systems and hardware
- Project Management
- Travel Time

Cybersecurity Consulting Services Total (T&M at $225/hour) $45,900*
**Estimated Travel & Living Expenses.....$2,004*
(Actual T&L expenses will be charged at cost +10%)

3.2 Pricing Assumptions

- Scope covers 188 hours of effort plus 16 hours for travel time and Project Management for a total of 204 hours commencing upon the agreed upon start date.
- Firewall rule analysis time will increase if there is no knowledge as to the origin of the firewall rules
- Specific control testing will not be performed in Phase 2 for the following areas: Account Management, Change Management, Patch Management, Vulnerability & Malware Management, and Security Logging and Monitoring per the defined scope established with CoA.
- The Cyber Security consulting will be limited to the active network components. Additional areas may be addressed subsequent to receiving a written change order to the associated purchase order.
- The consulting services are associated with the Process Control Network and are not applicable to the Business network except to the extent it connects to the PCN.
- Troubleshooting is not covered in this proposal.
- The assessment addresses the PCN from network operational and performance perspectives and will not address the Process Control System applications.

3.3 General Terms and Conditions

3.3.1 Proposal Terms

- This proposal is valid for through June 12, 2018
- All pricing and invoices in USD
- All local taxes, duties or tariffs are to be borne by the customer
- Upon acceptance of this proposal, customer will issue a purchase order that references this proposal number
- Pricing is for the stated scope of work; any changes will require a reissue of the proposal by PAS
- Scope changes will require a change order
- All payments shall be payable in accordance with the local government prompt payment Act 50 ILCS 505/4.
- Travel and Living (T&L) expenses are not included and will be billed at cost plus 10%, on-site services and travel to/from site includes $70 meals per diem.
- If customer, acting in good faith, disputes any invoiced amount, customer shall timely pay the undisputed amount. Upon resolution of any such dispute by the parties, customer will promptly pay any previously unpaid amount.
- Unless otherwise notified in writing by customer within forty (40) days of invoice date, PAS will regard the issued invoice as final and undisputed.
- This proposal is not to exceed $45,900 (plus expenses) without written consent from City of Aurora.

3.3.2 Payment Schedule

Services	
Monthly based on Actual work hours	$1,800 / 8-hour day

3.3.3 Procurement Information

Purchase Orders should contain the following:

Item	Description
Reference the Proposal Number	PL71114
Payment Terms	All payments shall be payable in accordance with the local government prompt payment Act 50 ILCS 505/4.
PO Number	Valid PO Number to bill against
Accounts Payable Contact	Accounts Payable Contact
Tax Exempt Status	Yes
Invoicing Instructions: (How are you expecting to be invoiced)	Please provide detailed invoicing instructions
Travel Expenses Invoicing Instructions	Travel and Living (T&L) expenses are not included and will be billed at cost plus 10%, on-site services and travel to/from site includes $70 meals per diem.
Bill To Address	Valid Bill to Address
Ship To Address	Valid Ship to Address
Scope of Work	• See section 2
Pricing Structure: • Lump Sum – one price for services + software + support + travel expenses • Fixed Price – one price for services + software + support (travel expenses billed separately at additional cost) • T&M – daily or hourly rate for services. Expenses billed separately at additional cost.	• T&M – daily or hourly rate for services. Expenses billed separately at additional cost.
PAS Fax	+1-832-645-7686
PAS Contact e-Mail	orders@pas.com
Postal Mail and Payment Checks to:	c/o: Account Receivable PAS Global, LLC 16055 Space Center Blvd., Suite 600 Houston, TX 77062 USA
Wire Transfers Payment:	All electronic wire fund transfers must include the company name, contract number and/or purchase or work order number, and invoice number. Details available upon request.

3.4 Project Delays

PAS reserves the right to charge a cancellation fee up to or equal to $5,940 for any on-site work cancelled with less than 7 days' notice. It is understood that last minute cancellations can directly impact PAS' delivery cost in the form of non-refundable airfares, travel re-booking fees, as well as associated resource management and scheduling activities. If customer suspends the project for more than thirty (30) days, PAS will invoice for all services completed prior to suspension date and required effort for demobilization.

3.5 Proposal Conditioned Upon Final Contract

If this proposal is for services work only, and not for the purchase of any software license(s), then this proposal is conditioned upon the final execution of a PAS Services Agreement.

3.6 Reference Documents

- 50 ILCS 505/4 (from Ch. 85, par. 5604)
    - Sec. 4. Any bill approved for payment pursuant to Section 3 shall be paid within 30 days after the date of approval. If payment is not made within such 30-day period, an interest penalty of 1% of any amount approved and unpaid shall be added for each month or fraction thereof after the expiration of such 30 day period, until final payment is made. (Source: P.A. 84-731.)

Appendix A: The PAS Advantage

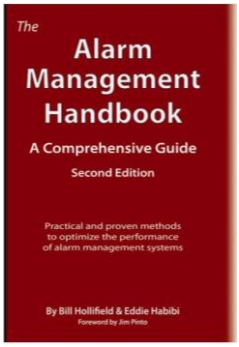
PAS is the leading provider of automation software for process safety, cybersecurity, and asset reliability to the power and processing industries worldwide. Our comprehensive portfolio includes solutions for industrial control system cybersecurity, automation asset management, and operations management which include alarm management, high performance HMI, boundary management and control loop performance management.

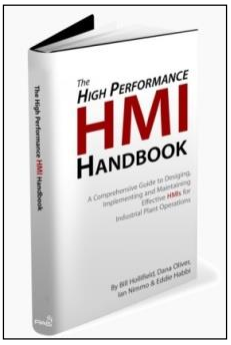
Cyber Asset Management	Operations Management
Secure critical operations by automating inventory and detecting unauthorized change for all major control systems – both proprietary and non-proprietary.	Improve process safety and profitability by providing greater operator situation awareness and avoiding unplanned production outages.
ICS Cybersecurity Inventory Management Configuration Management Patch Management Backup & Recovery Compliance Management	Alarm Management Boundary Management Control Loop Performance High Performance HMI

PAS is the global leader in Alarm Management and HMI Best Practices and as such, is committed to supplying solutions that minimize the total cost of ownership while maximizing value to our customers. The following areas detail the PAS Advantage through key differentiators.

Thought Leadership

For many years, PAS has been a thought leader in the field of alarm management and control loop performance management. We developed many best practices, which have become the industry norm for improving alarm systems and control loops. We participate in all of the industry knowledge development organizations and have helped craft the current group of important documents concerning alarm management.





Committee Member:

ISA 101 Human-Machine Interface

ISA 18.2 Alarm Mgt. Standard

EPRI Alarm Management Guidelines (Co-author)

RP-1167 Alarm Mgt for Pipeline Systems

Committee member

EEMUA 191

EEMUA Industry Review Group Member

Experience

Project Team

The PAS project team is the most experienced in the business. PAS has accomplished hundreds of successful projects in all industry segments around the world. PAS's level of experience in Automation Asset Management, Alarm Management, Cybersecurity, and High-Performance HMI is unmatched in the industry. PAS is vendor and supplier agnostic and provides a range of consulting services across almost all proprietary ICS systems. Our consultants have a wide range of skills and experience in both Information and Operational Technology disciplines.

PAS Solutions

ICS Cybersecurity

The architecture of Industrial Control Systems makes ICS configuration management critical. The timing and reliability requirements of ICS prohibit the use of traditional IT cybersecurity endpoint solutions commonly used on corporate IT infrastructure. Monitoring and maintaining a known configuration on control system assets are critical to maintaining the security and operational reliability. ICS configuration information is contained in multiple proprietary formats. Each ICS vendor uses different protocols on how and where data and information are stored. As a result, companies have come to realize that a uniform methodology to capture configuration management across multiple systems is a challenge. This belief has resulted in the maturity of the ICS configuration management process, which in comparison lags to the corporate IT side of the business.

PAS has developed Cyber Integrity™ as an enterprise application for automation asset management at industrial facilities. It aggregates and contextualizes configuration databases, programs and user interfaces, which facilitate risk management for multiple-vendor control systems in a single plant or across the enterprise. It also simplifies the visualization and management of information in automation systems improving operational reliability and security.

Automation Asset Management

Automation systems contain the collective knowledge of production and are critical to safe and profitable operations at industrial facilities. The automation system is the primary platform for continuous improvement and exposed to configuration changes on a regular basis. Additionally, an automation network typically includes systems from multiple vendors (DCS, SIS, APC, Historian, etc.), with each system containing proprietary databases and configuration, making it difficult for engineers to manage these highly integrated and complex systems.

Lack of up-to-date documentation and improper change management has been identified as a significant contributing factor to numerous industrial incidents and plant shutdowns. In a 2011 survey of automation professionals, more than 65% of participants indicated that their operations have experienced at least one incident in the prior twelve months due to unmanaged configuration changes to the automation system. Top tier power and process industry companies such as Dow, BASF, The Southern Company, Scottish Power, ExxonMobil, Shell, Aramco, and many others have identified lifecycle management of the automation asset a corporate priority.

PAS' Automation Asset Management is a comprehensive solution for proper lifecycle management of automation systems. Automation Asset Management is to control systems as physical asset management

is to pumps and compressors. It includes specialized software technology to facilitate a proven work process and the people whose job it is to ensure maximum availability of the automation assets throughout the lifecycle of the production facility.

PAS' Automation Asset Management is a vendor independent solution that aggregates, organizes, and presents simple visualization of complex automation configurations for the entire enterprise. It transforms the highly complex configuration of tightly integrated disparate systems into simple and intuitive visualization with significant drilldown capability.