Application Whitelisting Project Summary

Project Business Case

- Protection of process control data, networks, applications, and host operating systems, particularly in multi-vendor environments, is a critical, ongoing requirement for the Oil & Gas sector.

- A loss of control over a critical process potentially results in production loss, economic cost, environmental impact, facility damage, personnel injury, and loss of life.

- System maintenance increasingly centers on patching vulnerable automation software and operating systems, many of which have reached manufacture end-of-life, are unsupported by the vendor, and/or lack economic basis for replacement.

- This situation presents a formidable challenge to facility owners demanding process automation and environment reliability.

Host Protection Components

- **Anti-malware** (Virus, Trojans, spyware) solutions scan systems for executables matching known signatures.
- **Host Intrusion Prevention Systems** (HIPS) encompass a broad range of technologies including combination of behavioral monitoring, signature detection, host firewall, and application control.
- **Host Computer Firewalls**: A firewall examines communications between a given computer and the network and permits or blocks network packets based on a pre-defined rule-base.
- **Application Control/Application Whitelisting** (AWL) defines what applications are allowed to run and blocks everything else.
- **Memory Protection** is often offered with AWL solutions to prevent execution of unknown code that may be loaded into memory to bypass normal AWL execution prevention
- **Device Control** is offered with some AWL solutions to disable external devices (like USB)

© 2012 LOGIIC APPROVED FOR PUBLIC DISTRIBUTION

Anti-virus vs. Application Whitelisting

	What is bad ("black")	What is good ("white")
Policy (default) stance	Default-permit	Default-deny
Facility access example	No-access list (terminated staff, known criminals, etc.)	Access permission previously arranged for staff, others, etc.
Computer security example	Anti-virus	Application whitelisting
Main motivation	Easily finds bad things without impacting those not on the bad list	Tighter security because anything not explicitly listed as good is questioned
Main problem	All bad things may not be on the list (leads to "false negatives") permitting access/execution when it should not occur (e.g. malware executes or bad guys get access)	All good things may not be on the list (leads to "false positives") preventing access/ execution when it should occur (e.g. business disruption)

© 2012 LOGIIC APPROVED FOR PUBLIC DISTRIBUTION

Project Goal & Objectives

- **Project Goal**:
  Lower complexity, cost, and administrative overhead of host protection, without adversely impacting system reliability or performance.

- **Project Objectives**:
  - Determine how AWL integrates with current AV solutions
  - Understand best combination of host protection security solutions – AWL and AV
  - Assess how AWL solutions impact maintenance effort (e.g. AWL maintenance, OS and application patching, AV signature updates)
  - Understand feasibility of a single AWL solution that can support multi-vendor automation systems (which is a goal for some LOGIIC members)
  - Enable deployment of AWL solutions into automation environments by obtaining automation vendor accreditation
  - Verify the effectiveness of AWL solutions particularly to manage StuxNet-type and other zero-day attacks
  - Identify how AWL solutions can support various Legacy components (e.g. OS, process control systems)

Project Activities

Phase 1 – Technology Landscape

- Generate a short-list of technology/vendor candidates to participate in project
- Develop vendor selection criteria and test evaluation criteria

Phase 2 – Test Architecture and Facility

- Select a test environment consisting of typical assets found in ISA-99's reference architecture Level 2-3.5 zoned, windows-based test environment, instrumented with solutions representative of best-practice security
- Assemble and develop a test suite of malware and attacks of particular concern in automation environments

Phase 3 - Evaluation

- Evaluate solutions effectiveness by running a test suite against a baseline configuration (with AV and without AV) and candidate AWL solutions
- Evaluate AWL risks that effect automation processes (e.g. change mgmt)

Phase 4 – Project close

- Document "host protection" best practices, processes, and procedures with some relative measure of effort, ease of use, etc.
- Publish the base-line recommendations and practices

© 2012 LOGIIC APPROVED FOR PUBLIC DISTRIBUTION

LOGIIC AWL Evaluation Criteria

Show Stoppers	Other Considerations
Excessive Client installation time greater than 5 minutes	Effectiveness to prevent malware
Significant Air-gap (stand-alone) issues that prevent AWL management	Operational complexity: Easy of deployment and use of AWL
Negative performance impact (e.g. CPU) on BPCS (Basic Process Control System - specifically HMI)	Ability to apply solution into Installed Base and new projects
	Memory protection to prevent execution of unauthorized files
	Costs (deployment, operational) of AWL solution
	Automation vendor Accreditation/support of AWL solution(s)

© 2012 LOGIIC APPROVED FOR PUBLIC DISTRIBUTION

LOGIIC AWL Technical Approach

Assessment Methodology: R(*f*) = *T* x *V* x *C*

- Measured performance of technology by defined, realistic scenarios rooted in existence of a plausible (T) threat, existing (V) vulnerability, and observed (C) consequence.

Assessment Approach

- Clearly defined AWL, what it is, and what it is not
- Considered several constants in control system environment: the need for 24/7/365 uptime, operational situational awareness, unobstructed access to system during incidents, and life-safety criticality of data and control decision integrity

Analysis of Findings included consideration of data sources

- Baseline information gathered from technical scans, vendor documentation and discussion, and network reconnaissance
- Performance during technical red teaming and exploit response
- Observations during the assessment
- Usability testing
- Completion of functional test matrices
- AWL and automation vendor roadmap discussions were also considered

© 2012 LOGIIC APPROVED FOR PUBLIC DISTRIBUTION

Project Conclusions

LOGIIC Conclusions

- **AWL provides good protection against execution of files on systems, media, etc.**
  - AWL prevented Stuxnet in the lab (e.g. like before AV signature was developed)
  - AV is recommended to prevent executables with known virus
  - AWL provides protection when A/V signature and patches updates are infrequent

- **AWL addresses threats not addressed by AV or patching**
  - AWL may reduce criticality/frequency of AV updates, OS and app patches

- **AWL is most effective for systems that repeatedly perform the same functions with minimal changes** (e.g. static apps and functions)

- **AWL adds more value for older systems and increases in value as newer systems become older**
  - AWL is more effective on older OS (e.g. Windows2003/XP) vs. new OS (e.g. 2008/Win7) because new OS has up-to-date built-in security controls

- **AWL may be better suited for a subset of BPCS systems, rather than facility-wide deployment** (based on criticality of BPCS) – particularly when A/V is not practical

- **A single AWL enterprise solution is desirable.** However...
  - AWL vendors don't support some Install Base
  - AWL may not be cost effective or operational practical in some cases
  - Alternative Host Protection strategies may be appropriate in some cases

© 2012 LOGIIC APPROVED FOR PUBLIC DISTRIBUTION

Other AWL Benefits and Limitations

- **Other Benefits of AWL**
  - AWL creates an accurate inventory of your applications
- **Limitations of AWL**
  - AWL doesn't protect against all attacks
  - Some memory protection solutions require signature updates and/or custom rules
  - Maintenance and end of life for AWL solutions may present challenges in the future
  - AWL will trust all software delivered by a trusted updater
- **Benefits with Limitations**
  - Change Mgmt and Release Mgmt processes must be improved with AWL
  - Device Control can be a valuable tool to prevent introduction of files (e.g. USB)

© 2012 LOGIIC APPROVED FOR PUBLIC DISTRIBUTION

AWL Considerations

Selection Considerations	Configuration Considerations
Resource load on the system varies by memory protection product and/or Automation Application	AWL requires careful implementation and AWL policies
Effort required to interface AWL with AV	AWL must be implemented and maintained correctly
Your typical BPCS architectures and support capabilities vs. AWL solution requirements	Memory protection has limitations
Your legacy (OS) requirements vs. supported OS in AWL	AWL may conflict with AV, which may cause system to become unresponsive
Your functional requirements vs. AWL capabilities	
Your typical Asset Lifecycle for BPCS systems	
Your likely AWL overall cost of ownership for each solution	

AWL Testing Attributes

Testing Attributes	
Server Install	Works with common AV solutions
Client Install	Reboot Required?
Time to Whitelist	Works in an air-gapped environment
Protection against Conficker	Device Control
Protection against Stuxnet	Administration
Memory Protection	Ease of use with Vendor Architecture
File execution protection (zip, USB, etc.)	Ease of tuning with Vendor Architecture

Appendix B:
Project Background

© 2012 LOGIIC APPROVED FOR PUBLIC DISTRIBUTION

Project Out-of-Scope items

- Embedded Operating Systems, Non-Wintel, PLC/RTU's, and Field Devices
- Mobile/Portable/Hand-held devices
- Network Security Products (Firewalls, Intrusion Detection/Prevention, logging, Network Access Control (NAC)
- Provisioning, Patch & Configuration management products for OS & Control Apps and Security Compliance monitoring technologies and practices
- Software Assurance tools and techniques (app scanning, code review)
- Network Devices (router/switch/gateways, wireless)
- Encryption technologies, Data-loss prevention (DLP, data leakage)
- Non-commercially available, not-for-public release or research products
- Vendors/Technologies requiring confidentiality/non-disclosure agreements
- Security Vendors/products not reasonable available to Automation/Control systems
- SIS

© 2012 LOGIIC APPROVED FOR PUBLIC DISTRIBUTION

AWL Vendor Selection Weights

AWL Vendor Selection Criteria	Weight
Willingness to participate in an evaluation	20
Willingness to provide evaluation copy of software	20
Strategic alliances with automation vendors or integrators specializing in integration	20
Procedures for signature updates or whitelist modification, as appropriate to the technology	10
Engineer support for 2 days onsite and stand-by (phone) support at 3 sites	10
Alignment with project objectives	5
Roadmap going forward: technology and strategic alliances related to AWL	5
Interoperability with other standard security solutions	5
Other security capabilities can you provide in the process control environment	5
Candidates POSSIBLE Weighted Score	*100*

Automation Vendor Selection Weights

Automation Vendor Selection Criteria	Weight
Ability to provide a test facility for 2 weeks	20
Willingness to allow LOGIIC, SME, AWL vendors to test various attacks in test facility	15
Willingness to allow on network a Security Management Console and attack workstation	10
List of the OS and Process Control applications with patch levels in your lab	10
Process for certifying third-party security solutions; Willingness to accredit successfully demonstrated AWL solutions	10
Willingness to allow us to install other AWL software on your systems	8
Availability of an engineer to support the AWL test	8
Willingness to participate in an evaluation	5
Host security solution(s) in vendor's standard configuration(s)	5
Alliance with security solution providers	4
Vendor alignment with project objectives	3
Roadmap going forward: technology and strategic alliances related to AWL	2
Candidates POSSIBLE Weighted Score	*100*