



ACHILLES PRACTICES CERTIFICATION PROGRAM DESCRIPTION

Version 2.0 December 2010

Trademarks

Achilles™ is a registered trademark of Wurldtech Security Inc. in Canada and/or other countries.

Disclaimer

This document is produced and owned by Wurldtech Security Technologies and may not be copied, photocopied, reproduced, translated, or converted to any electronic or machine-readable form in whole or in part without prior written permission from Wurldtech. Wurldtech Security Inc. retains the right to change information in this document without notice.

Wurldtech Security Inc. believes the information in this document to be reliable and accurate but it is not guaranteed. Using and relying on this document is at your sole risk. Wurldtech Security Inc. is neither liable nor responsible for any loss, damage or expense arising from any omission or error in this document.

WORLDTECH SECURITY INC. GIVES NO WARRANTIES, EXPRESS OR IMPLIED. ALL IMPLIED WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT ARE DISCLAIMED AND EXCLUDED BY WORLDTECH SECURITY INC. IN NO EVENT SHALL WORLDTECH SECURITY INC. BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL OR INDIRECT DAMAGES, OR FOR ANY LOSS OF PROFIT, REVENUE, DATA, COMPUTER PROGRAMS, OR OTHER ASSETS, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

This document does not constitute a recommendation, endorsement or guarantee of any of the certified hardware or software products or the hardware and software used in certifying the products.

The certification does not guarantee that there are no defects or errors in the products. It does not guarantee that the products will meet your requirements, expectations or specifications or that they will operate without interruption.

This document does not imply any sponsorship, endorsement, affiliation or verification by or with any company mentioned in the document.

All trademarks, service marks and trade names used in this document are the trademarks, service marks and trade names of their respective owners. No endorsement, sponsorship, affiliation or involvement in either the certification, the document or Wurldtech Security Inc. is implied nor should it be inferred.

© 2010 Wurldtech Security Inc. All rights reserved.

Executive Summary

This document describes the Achilles Practices Certification (APC) program; it explains the general reference model, the certification program and the requirements for Bronze, Silver or Gold certification. The requirements set associated with each category of certification is determined by an industry agreement, not by an applicant for certification. Vendor-centric security requirements for process control are well defined by the International Instrument Users' Associations (WIB) in the report M2784-X-10 (version 2.0) dated October 2010.

Based on WIB's security framework requirements, end-user organizations, system providers and manufactures have engaged in a certification program to improve the quality of their cyber security processes and practices. The security requirements span from operations, to maintenance and support of an automation system (including Oil and Gas, electric and so on). They address all applicable processes embodied in organizational practices, system capability development, system acceptance testing and commissioning. These requirements are becoming prerequisites for delivery of a secure automation system.

Wurldtech Security Technologies expects to make minor adjustments in the tailored requirements to yield a suitable program for Vendor security certification in all critical infrastructure industries such as the Energy sector and Transportation sector. Nuclear facilities have special requirements that will require more extensive tailoring of the minimum requirements for Gold certification.

Wurldtech has developed the APC program to proactively and independently certify that Vendor's policies and practices build security into their products and services. There are three levels of certification:



Bronze certification verifies that a core set of applicable policies and practices are in place, enabled and practiced to build security into the Vendor's products and services.



Silver certification verifies that an extended set of applicable policies and practices are in place, enabled and practiced to enhance the security mechanisms built into the Vendor's product and services.



Gold certification verifies that a complete set of applicable policies and practices are in place, enabled and practiced to monitor and track performance of the Vendor's security mechanisms and improve those mechanisms through planned and resourced improvement programs.

Three APC documents are used to guide the Vendor towards a successful certification:

- APC Vendor Appraisal
- APC Vendor Submittal
- APC Vendor Report

Wurldtech oversees the applicant's execution of the Vendor Base Practices questionnaires and project lead interviews. For each certification level selected by the Vendor, this process yields the evidence needed to perform the security appraisal described in this document. When successfully completed, Wurldtech awards the objective Bronze, Silver or Gold certification.

Vendors displaying Bronze, Silver or Gold certification have demonstrated a well-defined level of security maturity practiced throughout the design, development, test, and maintenance of their products. These Vendors should be given competitive credit for building security into their products.

Table of Contents

1: Introduction

1.1: Scope	1
1.2: Intended Audience	1
1.3: Document Organization	1
1.4: Typical Questions Asked	1
1.5: APC Program Work Flow	2

2: Program Definition

2.1: Security Engineering	4
2.2: Introduction to the APC Program	4
2.2.1: APC for the End User	4
2.2.2: APC for the Vendor	5
2.3: Categories and Conformance	6
2.3.1: Process Area Categories	6
2.3.2: APC Program Conformance Requirements	7
2.3.3: APC Program Evidence	7
2.3.4: Policy Documents	8
2.3.5: Applicable Laws and Regulations	8
2.3.6: Measurements	8
2.3.7: Evidence Requirements Template	9
2.4: The Path to Certification	11
2.4.1: Certification Planning Phase	11
2.4.2: Preparation for Appraisal of Evidence	12
2.4.3: Evidence Collection and Appraisal	12
2.4.4: Report Findings for Certification	12

3: Program Documents

3.1: APC Program Description	13
3.2: WIB Security Requirements for Vendors	13
3.3: APC Vendor Appraisal Process	13
3.4: APC Vendor Submittal	14

3.4.1: Vendor Warrant 14

3.4.2: Qualifying Remarks 14

3.5: APC Vendor Sample Report 15

3.6: APC Vendor Pricing 15

Appendix A: Glossary

A.1: Terms and Definitions 16

A.2: Acronyms and Abbreviations 19

Appendix B: Bibliography

Appendix C: EWE Membership

List of Tables

Table 2-1: Process Area Categories	6
Table 2-2: Evidence Requirements Template	9
Table 3-1: Generic Questionnaire Template	13

List of Figures

Figure 1-1: Vendor Certification Work Flow	2
Figure 2-1: Certification Events	11

1 Introduction

1.1 Scope

This document describes the Achilles Practices Certification (APC) program; it explains the general reference model, the certification program, the requirements for Bronze, Silver or Gold certification, the types of evidence required, and the procedure and resources needed to achieve certification. It also includes a summary of other APC documents.

1.2 Intended Audience

This document is written for a Vendor or system integrator who wants to apply for certification. It describes the APC program and processes so the applicant can allocate the necessary resources to achieve certification. This document is intended for the applicant point-of-contact and technical lead responsible for resource management and certification performance.

1.3 Document Organization

This document contains the following chapters and appendices.

- Program Definition — Details the APC program and explains the four phases of certification.
- Program Documents — Summarizes each document used in the APC program.
- Appendix A: Glossary — Defines the terms used in the APC program.
- Appendix B: Bibliography — Lists a bibliography of source materials.
- Appendix C: EWE Membership — Lists EWE members.

For the convenience of the intended audience, a bibliography of source material is listed, terms used are defined and the certification program is defined in terms of the derived reference model, the certification process regarding what certification applies to and the steps taken by the applicant. Examples are included to highlight Vendor choices for certification.

1.4 Typical Questions Asked

This document is structured to answer several high-level questions. Other documents in the APC program set are structured to address the specific questions within the context of each document.

- What is the objective of the APC program?
- What is the expected result from successfully executing the APC program?
- How are the expected results characterized so as to be useful to the applicant?
- What expectations flow down to product suppliers and service providers?
- How much does it cost to execute the APC program?

1.5 APC Program Work Flow

Figure 1-1 illustrates the APC certification process work flow in terms of inputs, usage and outputs. It shows Vendor and Wurldtech activities and interactions.

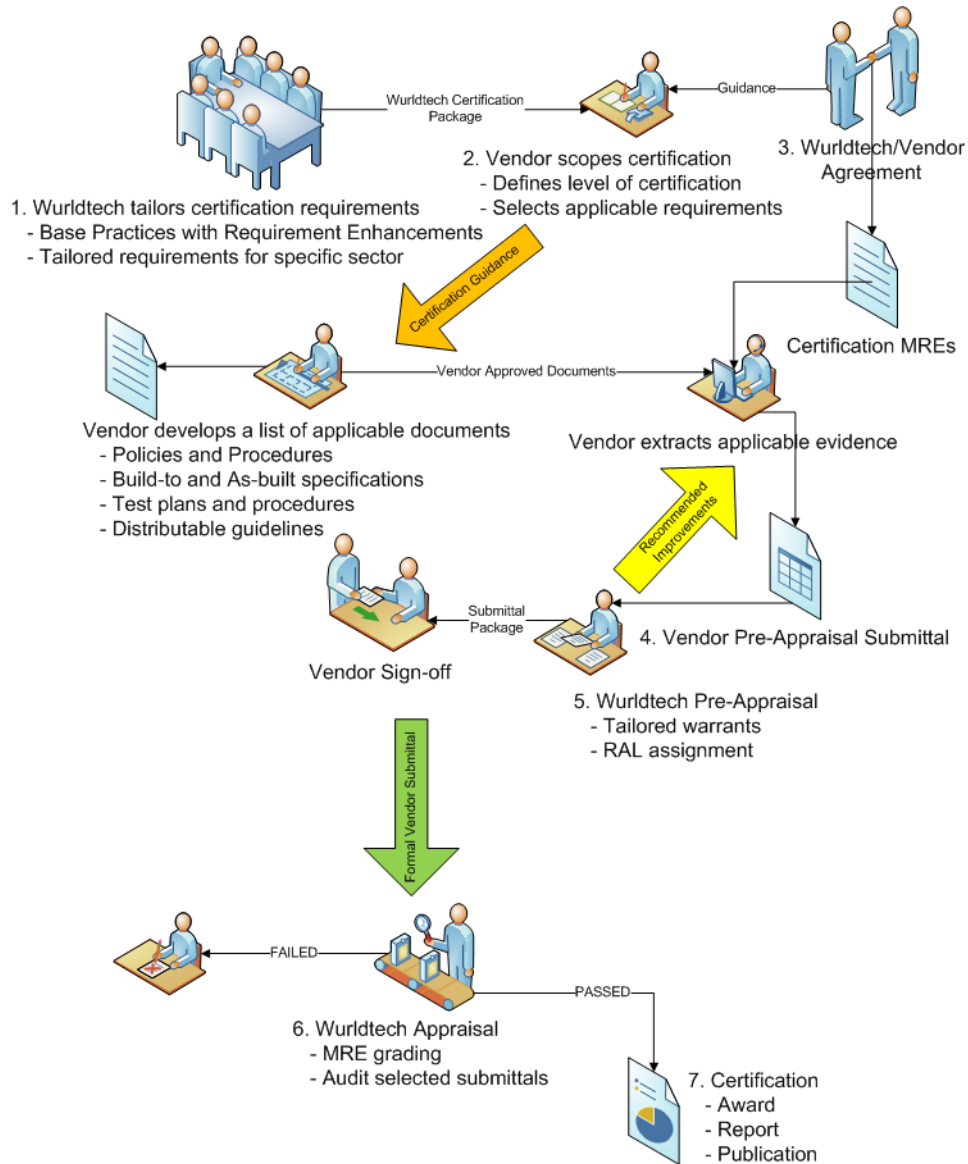


Figure 1-1: Vendor Certification Work Flow

- 1 Wurldtech prepares and sends a Project Pack containing APC program documents to the Vendor. For more information, see "Program Documents" on page 13.
- 2 The Vendor reviews the Project Pack. A Question & Answer (Q&A) Scoping Session is held between Wurldtech and the Vendor. Based on a mutual agreement between Wurldtech and the Vendor, applicable requirements are identified and a resourced Milestone Execution Plan (MEP) is established. Project execution is tracked against the milestone deliverables defined in the MEP.

- 3** During certification planning, and prior to gathering evidence for Vendor submittal, Wurldtech and the Vendor must agree to the scope of the certification with sufficient detail to avoid ambiguity. The declaration of scope does not contain requirements. Scope includes the following:
 - Declaration of the objective certification: Bronze, Silver, Gold.
 - Declaration of applicable Process Areas (PAs). In the case of a partial PA, there must be a declaration of applicable Best Practices (BPs) or qualification of the limit of applicability if required.
 - If equivalency is invoked, the Vendor must declare a list of equivalent approved documents that will be used as part of the evidence submittal. For example, version X document is applicable to version Y, where Y is the system considered for certification. Only the agreed-to list of equivalent documents is allowed for Vendor submittal of evidence. Documents not in the agreed-to list will be declared non-responsive.
- 4** The Vendor performs a self-appraisal. It is common practice for the Vendor to select at least one BP requirement from each process category, and to prepare the evidence submittal in response to the Minimum Required Evidence (MRE) specified in the APC Vendor Submittal [2].
- 5** Wurldtech performs a pre-appraisal of the sample Vendor submittals to ensure the MRE are understood and the submitted evidence is presented correctly. Wurldtech advises the Vendor of required changes to the evidence submittal for successful certification. The Vendor formally submits evidence for all applicable BPs to Wurldtech.
- 6** Wurldtech evaluates the submitted evidence using the Vendor Submittal [2] workbook (a macro-based EXCEL workbook) and assigns a pass or fail grade to each MRE. In the case of a fail grade, the appraiser assigns a Remedial Action Level (RAL) and provides some guidance for correction. The criteria for each RAL are as follows.
 - RAL=0: No action - Submission is graded PASS
 - RAL=1: Vendor editorial change is required to clarify, improve or correct the language of the submitted evidence. Technical content is correct.
 - RAL=2: Vendor fails to show that a required policy exists or is practiced and needs to develop the policy or put in place procedures to practice a required policy within 12 months from the date of certification. The Vendor can choose to tag the deficiency as a Pre-Planned Product Improvement (P3I).
 - RAL=3: Vendor system lacks the required APC program built-in security capabilities and needs to define a plan to provide the required capability within 12 months from the date of certification. The Vendor can choose to tag the deficiency as a P3I.
 - RAL=4: Vendor system fails to demonstrate the required APC program security capability and needs to correct the security function built into their system within 12 months from the date of certification. The Vendor can choose to tag the deficiency as a P3I.
- 7** Wurldtech prepares an APC report documenting all appraisal findings and recommendation. The Vendor reviews the APC report and, if necessary, submits clarification comments for Wurldtech to consider. If the Vendor disagrees with the grade of a specific MRE or the grade for certification, it may appeal the finding to the WIB Discretionary Board (WDB). WDB's ruling is final and cannot be appealed. When consensus is reached between Wurldtech and the Vendor, both parties sign the report approval block. Shortly thereafter, Wurldtech issues the APC program certificate and publishes the announcement of successful completion. All supporting documentation is securely archived by Wurldtech for future reference.

2 Program Definition

2.1 Security Engineering

At the most simple level, the risk process identifies and prioritizes security consequences inherent to a developed product or system. The security engineering process works with other engineering disciplines to determine and implement solutions to the problems presented by the consequences. The assurance process establishes confidence in the security solutions and conveys this confidence to the customers.

- Risk assessment is the process of identifying problems that have not yet occurred. As it is difficult to assess the likelihood of a system security threat, a more pragmatic approach is based on the potential consequences that result from the exploitation of a system security vulnerability.
- Security engineering, like other engineering disciplines, is a process that proceeds through concept, design, implementation, test, deployment, operation, maintenance, and decommissioning; the total life cycle of the system under consideration. The process of creating security solutions generally involves identifying possible alternatives and then evaluating the alternatives to determine which is the most promising. The challenge is how best to integrate this activity with the rest of the engineering process.
- There are many forms of assurance. One aspect is the confidence in the repeatability of the results from the security engineering process. The basis for this confidence is that a security certified organization is more likely to repeat results than an organization which is not certified. Wurdtech has adopted this basic concept for certification.

2.2 Introduction to the APC Program

Two perspectives are considered to introduce the APC program:

- An end user¹ is the entity or organization who legally owns the enterprise and may also operate the enterprise.
- A Vendor is an entity that provides, under contract to the end user, all goods and services specified in the contract. A Vendor may also integrate and manage the goods and services.

2.2.1 APC for the End User

The APC program evaluates Vendor security engineering processes according to how well they meet APC requirements.

Vendor security engineering processes are organized into four groups: Organization, System Capability, System Acceptance Testing and Commissioning, and Maintenance and Support. Certification of each group depends on the previous group. For example, if Organization processes conform to the stated requirements, they can be certified and the System Capability processes can be evaluated. If System Capability processes conform to requirements, the product/system can be certified (stating that it is configured in accordance with the requirements). The Testing and Commissioning processes can then be evaluated; if they comply to requirements, the Maintenance and Support processes can be evaluated and if they conform, the product/system can be certified (stating that it is tested, commissioned, operated and maintained in conformance with the requirements).

The logical groupings of security engineering processes are called Process Areas (PAs). Each PA is comprised of a set of Base Practices (BPs), which are evaluated to determine the APC certification of Bronze, Silver or Gold. In this context, the BPs form the requirements set for evaluation. If a process meets all applicable BPs at a particular certification level, it is awarded the corresponding Bronze, Silver or Gold certification.

¹.An end user is sometimes referred to as the Principal.

2.2.2 APC for the Vendor

The APC program requires that all Vendors comply with the WIB Security Requirements for Vendors [3]. The WIB document specifies requirements and provides cyber security recommendations to be fulfilled by Vendors of process control and automation systems to be used in an Automated System Domain (ASD). The APC program is accredited to demonstrate compliance with WIB requirements.

- End users must comply with their own security policies, standards and specifications for the ASD. These can vary with each end user. For this reason, the WIB requirements are a unified subset of the end user's security policies, standards and specification for the ASD. Vendors must comply with this subset of minimum requirements to receive certification.
- Vendors must document and inform the end user of any deviation their solutions may have from the WIB requirements. When deviations occur, the end user may require demonstration of the solution at the Vendor's premises or in a WIB approved laboratory as part of verification process that a solution is ASD security compatible.
- End users are encouraged to supplement the WIB requirements with a suite of end-user-specific design and engineering practices, specifications and/or guidelines that provide guidance on how to produce a ASD security compatible solution.
- If national or local regulations exist in which some requirements are more stringent than the WIB requirements, the Vendor must determine, by careful scrutiny, which requirements are more stringent and which combination of requirements is acceptable with regard to the safety, environmental, economic and legal aspects. In all cases, the Vendor must inform the end user of any deviation from the WIB requirements considered necessary to comply with national or local regulations. The end user may then negotiate with the national or local authorities concerned to obtain an agreement to follow the WIB requirements as closely as possible.

2.3 Categories and Conformance

2.3.1 Process Area Categories

Wurldtech has tailored thirty five (35) PAs to be used by Vendors applicants. These PAs are organized into four logical categories:

- Organization Process Areas
- System Capability Process Areas
- System Acceptance Testing and Commissioning Process Areas
- Maintenance and Support Process Areas

Table 2-1 lists the Process Area within each category.

Table 2-1: Process Area Categories

Process Area Categories	Process Area ID	Process Area Objective
Organization Process Areas	PA01	Prepare and Inform Personnel
	PA02	Designate a Security Contact
	PA03	Specify Best Practices
System Capability Process Areas	PA04	Harden the System
	PA05	Protect from Malicious Code
	PA06	Implement Patch Management
	PA07	Secure Account Management
	PA08	Support Backup/Restore
	PA09	Increase Network Visibility
	PA10	Standardize Historian Interfaces
	PA11	Verify Operations
	PA12	Connect Wirelessly
	PA13	Fortify Safety Instrumented System (SIS) Connectivity
	PA14	Provide Remote Access
	PA15	Protect Data
System Acceptance Testing and Commissioning Process Areas	PA16	Manage the Deployment
	PA17	Harden the System
	PA18	Protect from Malicious Code
	PA19	Implement Patch Management
	PA20	Secure Account Management
	PA21	Support Backup/Restore
	PA22	Implement the Architecture
	PA23	Connect Wirelessly
	PA24	Provide Remote Access
	PA25	Protect Data

Table 2-1: Process Area Categories

Process Area Categories	Process Area ID	Process Area Objective
Maintenance and Support Process Areas	PA26	Manage the Deployment
	PA27	Harden the System
	PA28	Protect from Malicious Code
	PA29	Implement Patch Management
	PA30	Secure Account Management
	PA31	Support Backup/Restore
	PA32	Implement the Architecture
	PA33	Connect Wirelessly
	PA34	Provide Remote Access
	PA35	Protect Data

2.3.2 APC Program Conformance Requirements

Each Certification Level consists of requirements that must be satisfied to be granted a Wurldtech certification of Bronze, Silver or Gold. The requirements set (including base requirement and requirement enhancements) associated with each level of certification is determined by an industry agreement, not by an applicant for certification.

For example, the PA01, BP.01.01BR, Bronze Level, states *"The Vendor shall ensure that personnel within its organization, subcontractors, and consultants who are assigned to activities of the Principal have been informed that the Vendor's Base Practices (see [3]) contains mandatory requirements for services or deliverables to the Principal."*

The WIB membership industries' agreement for certification includes three Requirement Enhancements (REs) which differentiate Bronze, Silver and Gold levels of certification.

- BP.01.01RE1(Silver): *"Vendor representatives shall enforce the process control security procedures specified in the Vendor's Base Practices (see [3]) and the Vendor's applicable security policies during engagement in activities on the Principal's site."*
- BP.01.01RE2(Silver): *"The Vendor shall have policies and procedures to support an incident response team led by the Principal."*
- BP.01.01RE3(Gold): *"The Vendor shall ensure that personnel within its organization, subcontractors, and consultants acknowledge and comply with security policies enforced by the Principal."*

A comprehensive list of all WIB membership industries certification compliance requirements is described in the Vendor Base Practices (see [3]). These requirements are aligned with the currently published NIST SP 800-53, ISA-99 and the NERC CIP requirements.²

2.3.3 APC Program Evidence

Evidence is commonly divided into two categories:

- Testimonial evidence includes statements or the spoken word from qualified security analysts and responsible organizational representatives.
- Real evidence includes policy documents, applicable laws and regulations, and measurement.

Testimonial evidence tends to be anecdotal or hearsay and therefore untrustworthy. For this reason, the APC program focuses on real evidence to support the Vendor's ability to accomplish a task.

²NIST SP800-53 is a relatively stable document. ISA-99 is a series of documents, most of which are a work-in-progress. The NERC CIP document is currently undergoing changes to strengthen the governance requirements.

2.3.4 Policy Documents

Within each PA, the APC program is designed to tally the existence of an applicant's policy documents that enable or support each goal objective which is articulated in the BP for that PA.

For example, PA01 in the Organization category, is 'Prepare & Inform Personal'. The stated goal is to ensure that security controls are properly used and configured. BP.01.01 is to 'Establish responsibilities and accountability for security control and communicate them to everyone in the organization.' When queried, the applicant answers in the affirmative that this requirement has been satisfied and offers the following evidence.

- Corporate policy identifying the responsible organization to write the applicable procedures and to monitor the performance of each organizational unit required to adhere to these procedures.
- List of written applicable procedures including document identifier, date of document and document author.
- List of Minutes of Meetings (MoM) including MoM identifier, date of the meeting, and name of the meeting facilitator. All members attending the meeting should sign acknowledgement forms that they have been properly briefed on the security requirements.

2.3.5 Applicable Laws and Regulations

Within each PA, the APC program is designed to tally the existence of applicable laws and regulations which support or impact the applicant's policy documents. When impacts occur, the differences must be reconciled to receive credit for certification.

2.3.6 Measurements

Real evidence, in the form of measurements, is considered in Silver and Gold certification. Silver certification focuses on project-level definition, planning, and performance issues. The Gold level of certification within each PA clearly identifies measurement requirements. The following list illustrates measurement requirements within PA01. The list is not complete but illustrates the correspondence between certification levels and measurement requirements.

- Silver: Establish responsibilities and accountability for security controls and communicate them to everyone in the organization. The following measurement evidence is required.
 - Percent of acknowledged distribution of security policies which includes assigned responsibilities.
- Silver: Allocate adequate resources (including people) for performing the process area. The following measurement evidence is required.
 - Percent of operational budget allocated within each participating organizational unit over the planning horizon associated with initialization, commissioning and maintenance.
- Gold: Tailor the standard process to meet the needs of a specific organizational unit's use. The following measurement evidence is required.
 - Within each participating organizational unit, the number of prioritized deviations required to meet the needs of their use. Prioritization may be as simple as 'must have' or 'nice to have.'
- Gold: Establish measurable quality goals for the work products of the organization's standard process family. The following measurement evidence is required.
 - Within each participating organizational unit, the percentage deviation from allocated resource budgets.
- Gold: Establish quantitative goals for improving process effectiveness of the standard process family, based on the business goals of the organization and the current process capability. The following measurement evidence is required.
 - Within each participating organizational unit, the slippage in meeting security milestones as related to planned dates.

Several important points are illustrated in the measurement requirements for PA01.

- A stated PA objective aligned with business goals provides a logical path through the certification levels. The objective of PA01 is to ensure that the intended security for the system is integrated into the system design.
- Measurement evidence must be stated as a cardinal number or percentage.

2.3.7 Evidence Requirements Template

Minimum Required Evidence (MRE) requirements for each BP are tabulated as shown in *Table 2-2*.

- **MRE ID** and **MRE #** contain the MRE identifier and number which associate the evidence requirement with a specific BP. The MRE ID is a concatenation of the BP.xx.yyBR or BP.xx.yyRE(z) and MRE #.
- **Evidence Requirement** contains a quantitative metric statement of the evidence.
- **Certification Level** indicates whether the evidence is required for Bronze, Silver or Gold certification.
- **Mandatory** and **Optional** indicate whether the evidence is mandatory or optional. Mandatory evidence requirements must be satisfied to achieve the objective certification award. Optional evidence requirements provide important information to assess the quality of the evidence, but are not required to achieve certification. Wurdtech expects many of the optional evidence requirements to become mandatory. Transition from optional to mandatory will be based on the results from pilot programs conducted within a specific industry sector.

Table 2-2: Evidence Requirements Template

MRE ID	MRE #	Evidence Requirement	Certification Level	Mandatory	Optional
BP.01.01BR	01	Vendor senior manager warrant certifying that personnel within its organization, subcontractors, and consultants who are assigned to activities of the end user have been informed of, and agreed to, the Vendor APC Base Practices mandatory requirements for all services or deliverables to the end user.	Bronze	X	
	02	Percent of total required acknowledged distribution of all security policies including assigned responsibilities to personnel. Note: Metric is a measure of enforcement to ensure compliance.	Bronze		X
BP.05.01BR	13	Percentage of Vendor's workstations, laptops, and handheld devices which have access to the Vendor's system that have up-to-date anti-virus software and signatures installed.	Bronze	X	
	14	Percentage of Vendor's servers which have access to the Vendor's system that have up-to-date anti-virus software and signatures installed.	Bronze	X	
BP.05.01RE(1)	15	Vendor senior manager signed warrant certifying the list of Vendor's system components not protected by anti-virus software and the procedures or mechanisms implemented to reduce the risk of infection.	Bronze	X	

Table 2-2: Evidence Requirements Template

MRE ID	MRE #	Evidence Requirement	Certification Level	Mandatory	Optional
BP.15.01BR	102	Vendor senior manager signed warrant certifying that the build to design requirements specification and the as built documentation for the Vendor's system describes the capability to protect selected data residing in any automated system repository from unauthorized access or use. Note: The objective is to provide the end user the means to enable protection of any named data object stored in an automated system repository.	Gold	X	
BP.15.03BR	104	Vendor senior manager signed warrant certifying that the build to design requirements specification and the as built documentation for the Vendor's system describes the capability to use encryption keys that provide at least 128 bit encryption.	Silver	X	

Note: The example shown in the evidence template is a sample of the evidence requirements for Certification of products and services in the WIB membership industries and the metrics in *“Measurements” on page 8.*

2.4 The Path to Certification

The procedures and resources required to achieve certification may vary because the APC program is tailored to an applicant's needs. Wurdtech has compressed the timeline used in the generic appraisal method by streamlining the detailed processes and procedures in the four phases of certification. *Figure 2-1* illustrates a milestone Gantt chart that describes each phase of certification. The example shows an applicant with geographically diverse organizational units and products, for whom certification will take approximately three months. The applicant certification events are shown above the timeline bar and the Wurdtech certification events are below. However, an applicant with a single, geographically centralized product could complete the four phases in one month.

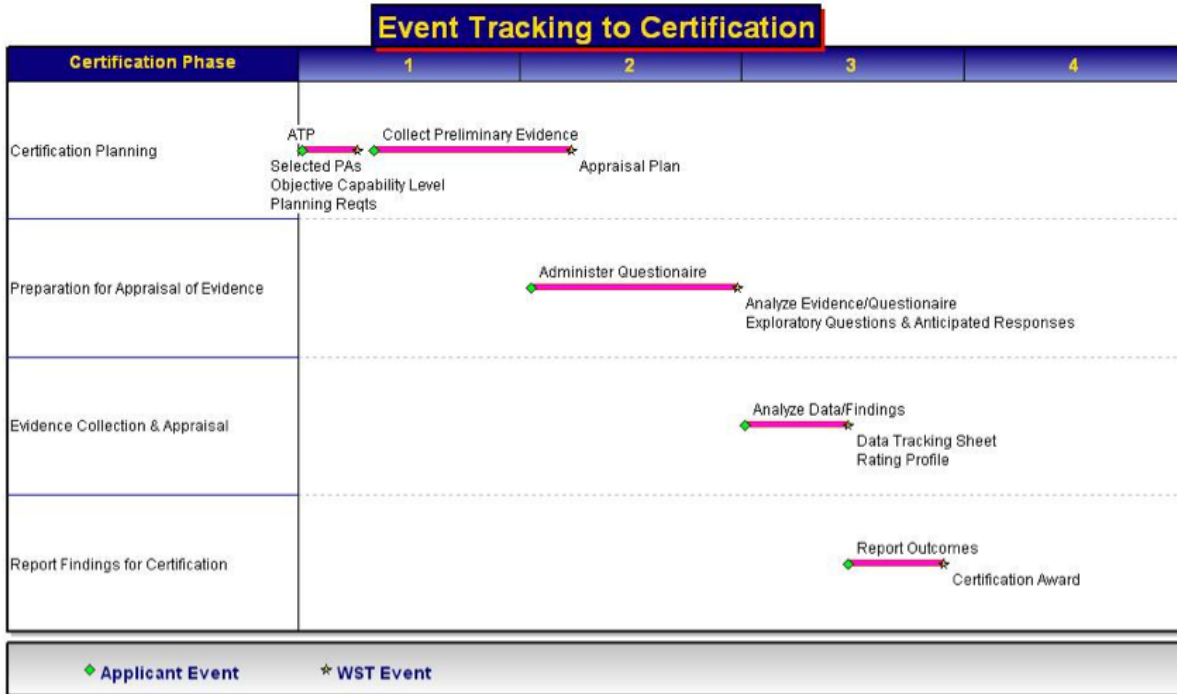


Figure 2-1: Certification Events

2.4.1 Certification Planning Phase

The Certification Planning Phase begins when the applicant receives authorization to proceed. The applicant establishes the purpose and goals of the appraisal, identifies the organizational units to be included, and selects the applicable PAs and objective Certification Level for certification.

Wurdtech uses this information to summarize the planning requirements and determine if preliminary evidence must be collected to complete the Appraisal Plan. If required, the applicant collects preliminary evidence from the organizational units and uses this data to tailor the reporting procedures, schedules and logistics.

2.4.2 Preparation for Appraisal of Evidence

Each participating organizational unit is assigned a set of PAs which are relevant to their operational responsibilities. A unit must answer a questionnaire and submit real evidence to support their claims.

There is a short timeline overlap between the end of the first certification phase and the beginning of the second phase which provides an opportunity to correct ambiguities and other planning parameters, and to update the Appraisal Plan if required.

Wurldtech analyzes the questionnaire responses and supporting evidence, and produces a set of Exploratory Questions and anticipated responses for the project lead interviews in the next certification phase.

2.4.3 Evidence Collection and Appraisal

Project leads from each organizational unit are interviewed, using the Exploratory Questions, to collect collaborating data about security engineering practices. The data is used to finalize the Data Tracking Sheet (DTS), which in turn is used to prioritize the appraisal findings for the selected PAs within the certification level.

2.4.4 Report Findings for Certification

Appraisal results are presented to voting applicant members for final edits and approval. With voted approval, Wurldtech awards the Bronze, Silver or Gold certificate for the selected PAs within the certification level.

3 Program Documents

3.1 APC Program Description

A description of the APC program. For more information, see “Scope” on page 1.

3.2 WIB Security Requirements for Vendors

The WIB has vetted a comprehensive description of the APC program requirements. The requirements set associated with each level of certification is determined by an industry agreement, not by a Vendor applying for certification.

Wurldtech has specified the evidence requirements for certification based on the minimum requirements for each PA. Each evidence requirement is assigned a unique identifier that can be used for cross-referencing and auditing to verify compliance with the requirements in the document.

3.3 APC Vendor Appraisal Process

A comprehensive description of the APC program requirements for the Vendor Appraisal Process and collecting the information required for certification. The questionnaires are administered to collect the evidence needed for appraisal. All questionnaires include the information shown in *Table 3-1*.

Table 3-1: Generic Questionnaire Template

Applicant Response				Remarks	Requirement Traceability						
QR#	Question Response				Evidence	MRE ID	MRE#	Evidence Requirement	Cert Level	M	O
	YES	NO	Don't Know								

When completing a questionnaire, the respondent answers “YES”, “NO”, “Don't Know” by checking the appropriate box. If the answer is YES, the respondent cites the evidence by referring to one or more document IDs. Each question is numbered so that the cited evidence can be verified against the BP requirements. The Appraisal Question column contains only those questions agreed to by the Vendor applicant during the certification planning phase. If evidence documents cited are related to one or more levels of certification, the evidence citation should be formatted to include the Certification Level: Document ID.

Evidence document is considered normative. Remarks are considered informative to qualify the normative evidence data and guide the appraiser to the appropriate section of a cited document.

3.4 APC Vendor Submittal

A comprehensive description of the APC program requirements for Vendor Submittal. Each MRE contains specific language describing the required information. For example, BP.15.01.02BR states

"Vendor senior manager signed warrant certifying that the build-to design requirements specification and the as-built documentation for the Vendor's system describe the capability to protect selected data residing in any automated system repository from unauthorized access or use. Note: The objective is to provide the Principal the means to enable protection of any named data object stored in an automated system repository."

3.4.1 Vendor Warrant

The format of the Vendor warrant is not specified in the APC program; it is determined by the Vendor. However, the warrant should include a warrant identifier for traceability, the date of the warrant, a description of the subject matter of the warrant, what it certifies, a list of documents supporting the claim made in the warrant, and signatures/date of the senior managers signing the warrant. The following is an example warrant for BP.15.01BR.

Warrant ID: OCGwarrantBP.15.01BR dated 2010-11-12

On behalf of OCG (the "Vendor"), I hereby represent and warrant that all of the information contained in the documents listed in this warrant provide the data needed to prepare an approved build-to design requirements specification and the as-built documentation for OCG's secure EMS/SCADA system version 9.1. The approved as-built documentation will be delivered with the system shipped to the Principal for System Acceptance Testing and Commissioning. After reasonable inquiry, the undersigned hereby certify that the security required to protect selected data at rest in any version 9.1 repository is adequately protected from unauthorized access and use. I am authorized by the Vendor to give this representation and warranty on behalf of the Vendor.

Applicable Documents:

- Approved EMS/SCADA system version 9.1 design specification dated 2010-03-31.
- Approved EMS/SCADA system version 9.1 interface requirements specification dated 2010-04-25.
- Interim approved EMS/SCADA system version 9.1 system acceptance test plans and procedures, dated 2010-08-31.
- OCG staffing approval sign-off for each document.

Warrant Signatures:

John H. Smith, OCG EMS/SCADA Program Manager. Dated: 2010-11-12

Note: Signature on file

3.4.2 Qualifying Remarks

Version 9.1 design specification and interface requirement specification describe role-based access control security requirements currently implemented in OCG's EMS/SCADA system. These security capabilities provided the necessary means for the end user to manage access and use control of all data residing in the EMS/SCADA system.

Version 9.1 system acceptance test plans and procedures are approved for factory acceptance testing to determine readiness to ship to the end user. Factory testing is scheduled for completion in December 2010. Changes required to the system acceptance test plans and procedures will be made and the approved as-built documentation delivered to the end user with the EMS/SCADA system.

Version 9.1 documents cited have been reviewed and approved by all responsible parties - see staffing signature block on each document.

3.5 APC Vendor Sample Report

A comprehensive description of the APC program requirements for the Vendor report. The Vendor Appraisal Workbook contains Vendor responses to each MRE and the Wurldtech appraisal findings and conclusions. The responses and findings verify that the APC program requirements have been met and adequately documented, and that a consensus vote regarding certification has been reached. The report includes a template for a Vendor senior manager signature and date approving the findings and summary conclusions, and a template for a signed and dated Wurldtech Certification Bronze, Silver or Gold award.

3.6 APC Vendor Pricing

A comprehensive description of pricing and resource requirements for Vendor participation in the APC program.

- The certification pricing model is a negotiated fixed price.
- The APC Vendor Pricing document provides a template and guidelines to estimate the Vendor provided resources required to execute the Vendor APC program. The template includes columns for estimating people time requirements for each step within the four phases of the appraisal process. The Vendor's resource commitment is marked up based on discussions with the Vendor's stakeholders and approved by the Vendor senior manager following an orientation meeting.

Appendix A: Glossary

A.1 Terms and Definitions

Term	Definition
Accreditation	<p>Formal declaration by a designated approving authority that a system is approved to operate in a particular security mode using a prescribed set of safeguards.</p> <p>Note: This definition is generally accepted within the security community, and is more constrained than the ISO Guide 2 definition.</p>
Assurance	<p>Degree of confidence that security needs are satisfied.</p> <p>Note: Assurance in the context of security is not considered to be an activity.</p>
Certification	<p>Procedure by which written assurance based on a comprehensive evaluation is given that system conforms to the specified security requirements.</p>
Compatible	<p>Capable of existing together in harmony.</p> <p>Note: A Vendor is compatible to end user's security policy and standards, when Vendor is compliant to this industry standard. The Vendor cannot be compliant to end user's policy and security standards, because part of this should be realized by the end user.</p>
Competency	<p>Capability for an individual to properly perform a specific job</p> <p>Note: Capability depends on skill which is defined as the capacity to carry out pre-determined results often with the minimum outlay of time, energy, or both.</p>
Compliance	<p>Adhering to, and demonstrating adherence to, a standard, regulation or agreement.</p>
Contractor	<p>Party that carries out all or part of the design, engineering, procurement, construction, commissioning or management of a project or operation of a facility.</p> <p>Note 1: The end user may undertake all or part of the duties of the Contractor.</p> <p>Note 2: A contractor may be a subcontractor/consultant (sometimes identified as a sub-vendor) to the Vendor who is responsible to the end user for all matters stated in the contract terms and conditions.</p>
Data link layer	<p>Protocol layer which transfers data between adjacent network nodes.</p> <p>Note: The Data Link Layer provides the functional and procedural means to transfer data between network entities and might provide the means to detect and possibly correct errors that may occur in the Physical Layer. Examples of data link protocols are Ethernet for local area networks (multi-node), the Point-to-Point Protocol (PPP), HDLC and ADCCP for point-to-point (dual-node) connections.</p>
Delegated technical authority	<p>Person who has received delegated authority from the end user to approve Derogations from the Process Safety requirements.</p>
Derogation	<p>Authorized variance or exemption from a Process Safety requirement, with specified conditions.</p>
Divulge	<p>To make public; to tell a secret so that it is generally known; to disclose.</p>
Effectiveness	<p>Property of a system or product representing how well it provides security in the context of its proposed or actual operational use.</p>

Term	Definition
End user	<p>Party that initiates the project and ultimately pays for its design and construction. Also known as Principal.</p> <p>Note: The end user will generally specify the technical requirements. The end user may also include an agent or consultant authorised to act for, and on behalf of, the end user.</p>
Equivalency	<p>Security functionality performs substantially the same way to yield substantially the same result.</p> <p>Note: Vendor may submit a document that applies to another product or another version of a product which is the target for certification with the stipulation that this document is applicable to the target for certification.</p>
Evidence	<p>Directly measurable characteristics of a process and/or product that represent objective, demonstrable proof that a specific activity satisfies a specified requirement.</p>
Host-based device	<p>Device running a general purpose operating system capable of hosting one or more applications or data stores.</p> <p>Note: Examples include human-machine interfaces (HMI), engineering workstations, historian servers, and domain controllers.</p>
Industry agreement	<p>Consensus for governance of the certification process and compliance requirements.</p> <p>Note: It is common IEEE and IEC practice to codify industry agreements as companion standard.</p>
IPSec	<p>Protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream.</p>
IT security	<p>Equivalent to process automated system cyber security and process automated system cyber security controls.</p> <p>Note 1: Derogation from these requirements SHALL [PS] be approved by the WIB.</p>
Network device	<p>Equipment that connects or manages network traffic: e.g., switches, routers and firewalls.</p>
Network layer	<p>Network layer which is responsible for end-to-end (source to destination) packet delivery including routing through intermediate hosts.</p> <p>Note: Whereas the Data Link Layer is responsible for node-to-node (hop-to-hop) frame delivery on the same link.</p>
Principal	<p>See <i>End user</i></p>
Procedure	<p>Written description of a course of action to be taken to perform a given task.</p>
Process	<p>Set of interrelated activities, which transform inputs into outputs.</p>
Process safety	<p>Management of hazards that can give rise to major accidents involving personnel safety, the release of potentially dangerous materials, and release of energy (such as a fire or explosion) or both.</p> <p>Note: The word SHALL [PS] indicates a Process Safety requirement.</p>
Quality goals	<p>Characteristics that define how a system is to be.</p> <p>Note 1: This should be contrasted with functional requirements that define specific behavior or functions.</p> <p>Note 2: Sufficient network bandwidth may also be a non-functional requirement, or quality goal of a system.</p>
Security	<p>Precautions taken to guard against crime, attack, sabotage, espionage, etc.</p> <p>Note: In this document, IT security is equivalent to process automated system cyber security, and process automated system cyber security controls.</p>

Term	Definition
Service set identifier (SSID)	Name that identifies a particular 802.11 wireless LAN.
Set point	A predetermined point within the range of an instrument where protective or control action is initiated.
System	<p>Discrete, distinguishable entity with a physical existence and a defined purpose, completely composed of integrated, interacting components, each of which does not individually comply with the required overall purpose.</p> <p>Note 1: In practice, a system is 'in the eye of the beholder' and the interpretation of its meaning is frequently clarified by the use of an associative noun, e.g. product system, aircraft system. Alternatively the word 'system' may be substituted simply by a context dependent synonym, e.g. product, aircraft, though this may then obscure a system principle perspective.</p> <p>Note 2: The system may need other systems during its life cycle to meet its requirements. Example - an operational system may need a system for conceptualization, development, production, operation, support or disposal.</p> <p>Note 3: When 'its systems' is used in APC program documents, it refers to all systems supplied and supported by Vendor over the systems lifecycle.</p>
Validation	<p>Meeting the needs of the intended end user.</p> <p>Note: See <i>Verification</i>.</p>
Vendor	Company that supplies or intends to supply an end user with equipment, or commissioning/maintenance services associated with equipment.
Verification	Reviewing, inspecting or testing to establish and document that a product, service or system meets regulatory or technical standards.
Warranty statement	<p>Guarantee that certain facets of an product or service sold is as factually stated or legally implied by the Vendor, and that often provides for a specific remedy such as repair or replacement in the event the article or service fails to meet the warranty.</p> <p>Note: Warrants used to certify correctness of security processes, policies, and procedures are considered legally enforceable and subject to liability settlements for negligence by the terms and conditions of the contract between parties.</p>

A.2 Acronyms and Abbreviations

ACL	Access Control List
AES	Advanced Encryption System
APC	Achilles Practices Certification
API	American Petroleum Institute
ASD	Automated System Domain
ATP	Authorization to Proceed
AV	Aniti-Virus
BP	Base Practice
BR	Base Requirement
BSI	British Standard Institute
CCR	Centralized Control Room
CIP	Critical Infrastructure Program
DACA	Data Acquisition and Control Architecture
DCS	Distributed Control System
DHCP	Dynamic Host Configuration Protocol
DMZ	De-Militarized Zone
DTS	Data Tracking Sheet
EICAR	European Institute for Computer Antivirus Research
EMS	Energy Management System
ER	Evidence Requirement
EWS	Engineering Work Station
FAQ	Frequently Asked Questions
FEP	Front End Processor
FIPS	Federal Information Processing Standard
HIDS	Host-based Intrusion Detection System
HMI	Human to Machine Interface
ICMP	Internet Control Message Protocol
ICS	Industrial Control System
ID	Identifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electric and Electronic Engineers
IP	Internet Protocol
IPS	Instrumented Protective System
IPSec	Internet Protocol Security
ISA	International Society for Automation
ISO	International Standards Organization
IT	Information Technology

L1	Network Level 1 - Basic Process Control
L2	Network Level 2 - Area Supervisory Control
L3	Network Level 3 - Site Manufacturing Operations Layer Note: Equivalent to the Process Control Network (PCN)
L4	Network Level 4 - Site Business Planning Note: Equivalent to the Office Domain (OD)
L5	Network Level 5 - Enterprise
M	Mandatory
MEP	Milestone Execution Plan
MIB	Management Information Base
MoC	Management of Change
MoM	Minutes of Meeting
MRE	Minimum Required Evidence
NERC	National Electric Reliability Corporation
NIST	National Institute Of Science and Technology
NTP	Network Time Protocol
O	Optional
OAGi	Open Applications Group industry
OD	Office Domain
OLE	Object Linking and Embedding
OLF	Norwegian Oil Industry Association
OPC	OLE for Process Control
P3I	Pre-Planned Product Improvement
PA	Process Area
PAS	Process Automation System (ICS, DCS, PLC, etc.)
PCAD	Process Control Access Domain
PCD	Process Control Domain
PCN	Process Control Network
PCS	Process Control System
PLC	Programmable Logic Controller
PtW	Permit to Work
Q&A	Question and Answer
RAL	Remedial Action Level
RDE	Remote Desktop Protocol Note: Used by Microsoft Terminal Services
RE	Requirement Enhancement
ROSI	Return on Security Investment
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition

SIL	Safety Integrity Level
SIS	Safety Instrumented System
SLA	Service Level Attainment
SNMP	Simple Network Management Protocol
SP	Special Publication
SSE	System Security Engineering
SSID	Service Set Identifier
SSL	Secure Socket Layer
T&C	Terms and Conditions
TCP	Transport Control Protocol
TPA	Third Party Access
USB	Universal Serial Bus
VPN	Virtual Private Network
WDB	WIB Discretionary Board
WIB	The International Instrument Users' Association - EWE
WMI	Windows Management Instrumentation
WPA	Wireless Protected Access (Note: WPA2 has replaced WPA)
WSUS	[Microsoft] Windows Server Update Services

Appendix B: Bibliography

- [1] Wurldtech Security Technologies, *Achilles Practices Certification - Vendor Appraisal Process*, Guideline, Work-in-Progress.
- [2] Wurldtech Security Technologies, *Achilles Practices Certification - Vendor Submittal*, Guideline, Work-in-Progress.
- [3] International Instrument Users' Association, *Process Control Domain - Security Requirements for Vendors*, WIB Working Group: Plant Security, The Netherlands, Report Version 2.0 (Index Classification 50.1) M 2784 X10, October 2010.

Appendix C: EWE Membership

EWE is the International Instrument Users' Association; a consortium of Evaluation International (EI), WIB and EXERA. The following is a list of EWE members dated March 2010.

Acetex Chimie	IRA
Adisseo	KEMA Nederland BV
Aeroport de Paris	Kuwait Petroleum Europoort BV
Agence de L'Eau Artois Picardie	Laborelec
Air Liquide	Lanxess
Akzo Nobel T&E	LNE
Aramco Overseas Company BV	Lubrizol France
AREVA	Lyondell Basell
Arkema	Magnox Electric Ltd
AWE	M+W Process Automation
Axens	Nantes Metropole - Direction de l'Eau
BAE Systems	Nederlands Meetinstituut-NMi
BP PLC	NPL Management Ltd
BP Refinery Rotterdam BV	Petro SA
British Energy plc	Polimeri Europa
CETIAT	RATP
Chiyoda Corporation	Renault SA
C&Tsi	RHODIA
DCNS	Rolls-Royce Submarines
DGA	SABIC Europe BV
DOW Benelux	SANOFI PASTEUR
DSM BV	Schering-Plough Corp.
Du Pont de Nemours BV	Sellafield Ltd
EADS/AIRBUS	Shell Global Solutions International BV
EDF	ShinEtsu-PVC BV
ENEL Generazione	Sicilaque
EniACQUA CAMPANIA	SIP Standardiserad Instrumentprovning
ExxonMobil USA	Solvay SA
GDF	Suez Environnement
Health & Safety Executive	Total
Heineken SCS	Università di Genova
IGR	Università di Pisa
INEOS	Urenco ChemPlants-Ltd

INERIS	Véolia eau
INRS	Waternet
Intertek Polychemlab	Wintershall Noordzee BV

Wurldtech Security Technologies

For more information about Wurldtech Security Technologies contact:

Wurldtech Security Technologies, Inc.

401 W Georgia Street, Suite 1680

Vancouver BC Canada

V6B 5A1

Tel +1 (604) 669 6674

Fax +1 (604) 669 2902

Email info@wurldtech.com

We also invite you to visit our website at:

www.wurldtech.com

