History Part I

The WIB – A Collection of End Users

The Werkgroep Instrument Beoorderling (WIB), or the international instrument users association

Comprised of over 50 end-users from various industrial sectors located around the world

Collaborate to solve various manufacturing challenges

History

- Founded In 1962 (The Netherlands)
- 75+ Global End-user Members
- Plant Security Sub-working Group led by Shell cyber security team
The WIB Storyline: From Concept To Standard

NERC/CIP, CFATS,
DHS Procurement Language, ISAPS99,
NIST 800-53, ISO 2700x, NIST IR 7628 etc, etc, etc.

First industry driven standard

Select the low hanging fruit
The WIB security requirements

The WIB Plant Security Working Group (PSWG) announced version 2 of the security requirements for Vendor’s in November 2010

- 2 versions with 4 revisions
- 50+ stakeholders: vendors, end-users, consultants, subject matter experts
- Over 1000 comments/change requests
- Aligned To IEC framework for future adoption (IEC 62443-2-4 approval pending)
Comparison of security assurance

Objective Security Assurance

Certification Requirements

- IEC62531
- IEC Parent Systems

FR – Foundational Requirements
SR – System Requirements
History Part II
Alignment with ISA99 & NISTIR 7628
APC and ISASecure

- APC (Achilles Practices Certification) is the certification program currently in place to assess conformity with the WIB requirements, which focuses on vendor security practices. It is currently managed by Wurltdtech Security Technologies, under approval from the WIB.

- ISASecure is the certification program managed by the ISA Security Compliance Institute to assess conformity with selected parts of the ISA99 Standards Roadmap. The first ISASecure product is the Embedded Device Security Assurance (EDSA) Certification, which focuses on device security characteristics.

- Both programs are complementary to each other.

- Both programs are continual works in progress.

- Both programs serve the security needs of the community TODAY.
This is the workspace for the IEC 62443-2-4 Task Force

- Lead: Mike Ahmadi (mike.ahmadi@granitekey.com)
- The Group Mailing List address for the Task Force is the same as the HLR mailing list address: csctgrmtsa@nist.gov (email marianne.swanson@nist.gov and tanya.brewer@nist.gov to be added to the group)
- Meeting Info: Fridays, 4-5 PM Eastern
- Dial In: 1-800-728-9607 (Toll Free), 1-917-904-9873 (Direct), Participant Passcode: 4570752
- The collaborative Google Doc is available by following this link: https://docs.google.com/document/d/1v3MVYx_ZXp9MozolYwcxcNn3jmDhCNZ5Vb2W3crXknU4/edit?hl=en_US&authkey=CfIEo84h+#. Please put your name in the Attribute column and add your comments. Do not alter anyone else's comment. [THE COMMENT PERIOD FOR THIS DOCUMENT IS CLOSED]
- Due to potential copyright issues, we will not host any IEC 62443 series documents on this site. Please contact Tom Phinney at tom.phinney@cox.net and he will provide you with the relevant IEC draft documents.

To join, please contact Tanya Brewer (tanya.brewer@nist.gov).

- WIB_2.0_-_NISTIR_7628_Alignment_2011-03-16.pdf: WIB 2.0 and NISTIR 7628 Alignment Document
- WIB_2.0_-_NISTIR_7628_Alignment_2011-03-16.pdf: WIB 2.0 and NISTIR 7628 Alignment Document
UCAIug OpenSG

Security Conformity Task Force

- Task force formed under OpenSG to address security conformity
- Could serve as adjudicator for member organizations

2.0 Scope

The overall scope of the Smart Grid Security Testing Council is to organize the effort for identifying and adapting a Smart Grid Security Certification guideline and Smart Grid Security Assessor Certification guideline (refer to Organizational Structure below). The certification guideline describes an ongoing process that demonstrates the information security maturity of a vendor product and service over time.

2.1 Certification Scope

The goal of the Smart Grid Security Certification is to ensure:

- Security tests are conducted routinely (annually) against approved predefined tests and are properly executed to produce expected results
- Security tests are performed by independent agents not affiliated with either the product being tested or the entity requesting the test
- Security tests comply with laws and regulations
- Security tests provide sufficient coverage, i.e., includes all components necessary to represent the system under evaluation (holistic)
Enormous Outpouring of Participation In IEC Project

- Over 50 participating organizations from public, private, and academic sectors
- Participation from major countries (including US, China, Japan, Holland, France, Switzerland, Germany, Brazil...and many more)
- Over 1000 comments
From Requirements To Vendor Certification

- Build on WIB 2.0
- Blessed by PSWG

- Over a year of pilot programs
- Multiple vendors
- Various industry sectors

- Scalable certification program
- Internationally accepted frameworks
- Formal, testable criteria

- WIB accredited November 2010
- 1st certified vendor January 2011
Scalability: the certification levels

**Bronze certification:** 148 of 272 Requirements
Entry-level certification, awarded for successful completion of all applicable requirements for security policies and practices that have been implemented and verified through direct measurement or analysis.

**Silver certification:** 218 of 272 Requirements
Awarded for successful completion of all applicable requirements and selected requirement enhancements that have been implemented and verified through direct measurement or analysis.

**Gold certification:** 272 of 272 Requirements
Awarded for successful completion of all applicable security policies and practices that exist in a vendor’s system. Gold level contains additional performance and industry-specific requirements.
The requirements framework

- Organization
- System Capability
- System Testing & Commissioning
- Maintenance & Support
| PA01: Prepare and Inform Personnel | BP.01.01: Requirement recognition and enforcement | BR: 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 Base Practices (this document) contains mandatory requirements for all services or deliverables to the Principal. Note: Terms and Conditions (T&C) for subcontractor and consultant contracts and purchase orders should include a requirement to adhere to the WIB standards and practices. | Bronze |
| RE(1): Vendor representatives shall enforce the control system security procedures specified in this document and the Vendor’s applicable security policies during engagement in activities on the Principal’s site. | Silver |
| RE(2): The Vendor shall have policies and procedures to support an incident response team led by the Principal. | Silver |
| RE(3): The Vendor shall ensure that personnel within its organization, subcontractors, and consultants acknowledge and comply with security policies enforced by the Principal. | Gold |

**Organizational process area**

- **Category Description:** Requirements and Enhancements targeted at organization policies and procedures
- **Conformance Criteria:** Proof of policy existence and evidence of its application
<table>
<thead>
<tr>
<th></th>
<th>BP.06.02: Patch qualification</th>
<th>BR: The Vendor shall qualify all relevant software patches and service packs for use on its system during its supported lifetime including security patches that are released by the manufacturer of the operating system and third party software used on their system. Note: Patch testing and qualification, and more importantly deploying necessary patches should follow the guidelines offered in ISA-99.02.03.</th>
<th>Bronze</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>RE(1): If a security patch is considered not relevant by the Vendor for use on its system, the reason shall be provided to the Principal.</td>
<td>Bronze</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RE(2): If a security patch is not approved by the Vendor for use on its system, then the reason and remediation plan shall be provided to the Principal. The remediation plan shall describe how a solution will be provided within 12 months.</td>
<td>Bronze</td>
</tr>
</tbody>
</table>

**System capability process area**

- Category Description: Requirements and enhancements for security functions to be designed into the Vendor’s system and compensating security functions used to protect Vendor’s system components and subsystems which do not have built-in security capabilities
- Conformance Criteria: Proof of system capability and verification of functionality
<table>
<thead>
<tr>
<th>PA19: Implement Patch Management</th>
<th>BP.19.01: Up-to-date systems</th>
<th>BR: For systems maintained by the Vendor, the Vendor shall keep the security patch levels of all ASD systems current to within 3 months of the security patch being available and qualified by the respective system Vendor.</th>
<th>Bronze</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>RE(1): If the installation of patches requires an outage that can impact operations or impacts performance, the Vendor shall develop and document a mitigation plan subject to approval by the Principal.</td>
<td>Bronze</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RE(2): Vendor approved patches shall be approved by the Principal before they are installed on the Vendor’s system.</td>
<td>Bronze</td>
</tr>
</tbody>
</table>

System testing and commissioning process area

- Category Description: Requirements and enhancements for demonstrating correct implementation of security functions built into the vendor’s system, and readiness of system turnover for operation by the Principal or his selected Operator
- Conformance Criteria: Verification of security functionality and existence of operational polices
<table>
<thead>
<tr>
<th>PA28: Protect from Malicious Code</th>
<th><strong>BP.28.01:</strong> General anti-virus policy</th>
<th>BR: Prior to scheduled maintenance, the Vendor shall update the document describing the configuration of the virus detection software installed on each ASD component.</th>
<th>Bronze</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>BP.28.02:</strong> Portable media procedure</td>
<td>BR: Prior to schedule maintenance the Vendor shall update documents describing changes to a procedure for its staff stating that portable media (e.g. laptops and USB storage) used by the Vendor for commissioning and maintenance of equipment or devices in the ASD are used for this purpose only.</td>
<td>Bronze</td>
</tr>
<tr>
<td></td>
<td><strong>BP.28.03:</strong> Anti-virus management</td>
<td>BR: Prior to scheduled maintenance, the Principal shall document changes to the installation of virus definition files have been installed and verified within 30 days after being qualified by the system Vendor.</td>
<td>Bronze</td>
</tr>
</tbody>
</table>

**Maintenance & support process area**

- Category Description: Requirements and Enhancements for demonstrating correct maintenance of security functions built into the Vendor’s system, and timely support in response to security related events
- Conformance Criteria: Existence of policy and its application and verification of functionality.
The Certification Process

**Scoping – the key to success**
Certification scope and planning
Define applicable requirements & exceptions

**Preparation – vendor heavy lifting**
Vendor self-appraisal, collecting evidence & warrants,
Assessor quick review

**Appraisal – scoring the evidence**
Vendor submits final data
Assessor review & request evidence and clarification

**Reporting – the finish line**
Collate findings, observations and recommendation
Certificate issue.
The cost of certification is recoverable

- Successfully completing FAT & SAT is required to deploy, operate and maintain the process control system.
- Given the requirements to operate securely, security testing must be an integral part of FAT & SAT.

Analysis shows the reduction in cost realized if Vendor is security certified 40%-75%; test plans, procedures are in place to satisfy certification.

Vendor not certified must develop and exercise proper security test plans and procedures – this cost is well defined.