

## Overview

### Achilles Certification

The Achilles Certification Program was developed by Wurdtech and its partners to provide a benchmark for the deployment of secure industrial devices. The program is designed to assess the network robustness of industrial devices and certify that they meet a comprehensive set of requirements and conformance. The certification process presents device manufacturers with an independently verified result from which to communicate their product security to customers, while providing the operators of control systems with the most complete, accurate, and trustworthy information possible about the network resilience of their deployed products.

### Host-Based Devices

As proposed by ISA99, a host-based device (HBD) is a general purpose device running a general purpose operating system capable of hosting one or more applications or data stores. Examples include human-machine interfaces (HMIs), engineering workstations, historian servers, and domain controllers.

## The Certification Process

### How are devices tested?

The certification tester can test the device-under-test (DUT) in one of three ways:

- **On-site.** The tester goes to the customer's site with an Achilles™ Satellite and performs the testing.
- **Locally.** The customer sends the device to Wurdtech and the tester performs the tests locally.
- **Remotely.** The Satellite and the DUT are at the customer's site and the tester runs the tests remotely.

### How much time is required for testing?

Three days.

### When should a device be submitted for testing?

Achilles Certification is tied to the specific version numbers of the software programs running on the HBD. Therefore, the customer should submit an HBD for testing only when it and its software programs are final and ready to be released to market.

### What do I receive when a device gets certified?

If the device achieves certification, the customer receives a detailed report that describes the test procedure and test results; a certificate; inclusion in the list of certified devices on the Wurdtech website; and use of the Achilles Certification logo.

## Test Methodology

### An HBD has many components (the operating system, device drivers, software programs). What part of the HBD is being certified?

Achilles Certification of an HBD certifies:

- Vendor modifications to the operating system's network stack.
- Network services running on the HBD.

### What kinds of tests are run against the HBD?

The tests executed by the Achilles Satellite fall into two categories:

- **Resource Exhaustion Tests.** Tests that try to exhaust a particular resource of the DUT. For instance, the Achilles Satellite employs storms, which are tests that send packets at fast rates in an attempt to overflow the DUT's memory resources.
- **Invalid Packet Tests.** Tests that send illegally-formed packets to the DUT. The Achilles Satellite uses fuzzers and grammars to create these invalid packets.

### What protocols are tested?

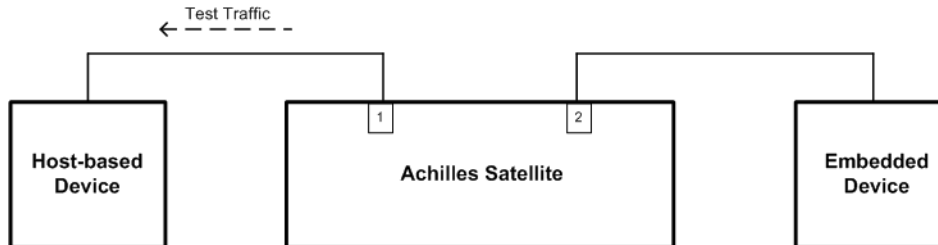
The Achilles Satellite offers a wide range of tests for various network protocols. Wurdtech categorizes these protocols into four separate categories:

- Level 1. Common protocols found in layers 2-4 of the OSI model.
- Control. Protocols that are specific to industrial control.
- Proprietary. Closed protocols that are specific to a vendor.
- Other. Protocols that do not belong to one of the other three categories.

To achieve Achilles Certification, the HBD must pass the Level 1 tests. Tests for other protocols are optional. However, for these optional protocols, Wurdtech will communicate which protocols have been certified, as will be explained on the next page.

## Test Methodology (continued)

What does the test bench look like?



The Achilles Satellite is connected inline between the HBD and its associated embedded device (which may be a PLC, SIS or DCS controller, etc). The two ports on the Achilles Satellite, Ports 1 and 2, are bridged so that all traffic from the HBD continues to reach the embedded device and vice versa. Test traffic is sent from Port 1 to the HBD only. The embedded device is included in the test bench to more closely resemble a real operating environment.

What are the certification conformance requirements?

The Achilles Satellite determines test results through Monitors, which monitor some particular characteristic of the DUT. Four of these monitors are used to determine certification compliance:

- ICMP Monitor; TCP Ports Monitor; UDP Ports Monitor. Monitors the status of the network stack during testing.
- Windows/Linux System Monitor. Monitors the status of the processes and resource utilization on the HBD.

The ICMP Monitor/TCP Ports Monitor/UDP Ports Monitor must all remain Normal during invalid packet tests. For resource exhaustion tests, the three monitors may go into Warning but must recover immediately after the test ends. The Windows/Linux System Monitor must remain Normal throughout all tests.

## Example Certified Device

The Wurldtech website will display information on certified devices as depicted on the right. The Product Details portion of the table lists device details such as device vendor and device category, as well as certification details such as the date certified.





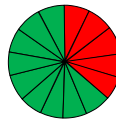
The Protocol Coverage part of the table shows which of the device's protocols have been Achilles Certified. Assume that the device described in our example supports three control protocols, four application protocols, and one proprietary protocol. Assume that it passed the Level 1 test suite; that it passed the Modbus/TCP and MMS control protocol tests; that it passed the HTTP application protocol test; and that no proprietary protocols were tested.

The pie charts illustrate what portion of the category's attack surface has been certified. Green slices represent certified protocols; red slices indicate uncertified protocols. In our example, Device X has three control protocols, but only two have been certified. Therefore, the control protocol pie chart is 2/3 green and 1/3 red. Each certified protocol is listed in the appropriate cell, and note how uncertified protocols are not explicitly named.

By providing this level of detail into which individual protocols have achieved certification, end users can compare certified devices and choose the most suitable device for their needs. Furthermore, Wurldtech will provide a ranked list of all certified devices, ranked by the percentage of protocols certified, thereby differentiating and rewarding devices according to their overall network robustness.

## Contact Information

If you would like to schedule a certification or if you would like more information, please contact us at [certifications@wurldtech.com](mailto:certifications@wurldtech.com).

Product Details		Protocol Coverage	
<b>Vendor</b>	Vendor A	<b>Level 1</b>  6/6	802.3, ARP, ICMP, IP, TCP, UDP
<b>Category</b>	Host-Based Device	<b>Control</b>  2/3	Modbus/TCP, MMS
<b>Product</b>	Device X	<b>Proprietary</b>  0/1	
<b>Software Versions</b>	HMIsoft 1.3 HMIServer 2.4	<b>Other</b>  1/4	HTTP
<b>Operating System</b>	Windows XP SP 2	<b>Overall</b>  9/14	
<b>Date Certified</b>	6/12/2009		
<b>Notes</b>	Tested at WST Labs		
<b>Exceptions</b>	None		