achilles CERTIFICATION

# *Achilles Level 1 Certification Requirements for Host-Based Devices*

## Host-based Device Definition

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.

## Pass/Fail Criteria

Host-based device certification is currently supported for HBDs that run Windows or Linux. Depending on which OS is run by the HBD, different Achilles Satellite Monitors are used to determine certification pass/failure. The OPC Monitor is used to observe the performance of Windows machines, whereas the Linux System Monitor is used to observe the same for Linux machines. In addition, the ICMP Monitor, TCP Ports Monitor, and UDP Ports Monitor are used to observe the networking behavior of both Windows and Linux HBDs. The monitors determine pass/failure as follows:

Both Windows and Linux:

- The ICMP Monitor:
  - must remain Normal during invalid packet tests.
  - may go into Warning for resource exhaustion tests, but must recover before the test ends, i.e., the monitor outcome must not be Failure.
- The TCP Ports Monitor:
  - must remain Normal during invalid packet tests.
  - may go into Warning for resource exhaustion tests provided that the ICMP Monitor is also in Warning, but must recover before the test ends, i.e., the TCP Ports Monitor outcome must not be Failure.
- The UDP Ports Monitor:
  - must remain Normal during invalid packet tests.
  - may go into Warning for resource exhaustion tests provided that the ICMP Monitor is also in Warning, but must recover before the test ends, i.e., the UDP Ports Monitor outcome must not be Failure.

Windows Only:

- The OPC Monitor:
  - must remain Normal during invalid packet tests.
  - may go into Warning for resource exhaustion tests provided that it is the *"Processor(_Total).ProcessorTime < 100"* (see below) condition causing the Warning state. The monitor must recover before the test ends, i.e., the OPC Monitor outcome must not be Failure.

Linux Only:

- The Linux System Monitor:
  - must remain Normal during invalid packet tests.
  - may go into Warning for resource exhaustion tests provided that it is the *"CPU Usage (%)"* (see below) condition causing the Warning state. The monitor must recover before the test ends, i.e., the Linux System Monitor outcome must not be Failure.

All tests are executed at or below 10 percent link utilization. For example, on a 100 Mbit link, all test cases are executed at 10 Mbits/s or below. If any of the above criteria are not met for a single test case, then the DUT fails Achilles Level 1 Certification.

### Pass/Fail Criteria Exceptions

If any of the pass/fail criteria are not met, an exception may be granted if the device under test's (DUT's) behavior is due to an explicit design decision. For instance, perhaps the network stack is designed to stop responding to traffic for 60 seconds if it detects that it is receiving a large amount of invalid traffic. Such behavior will likely result in the DUT not sending ICMP replies to the Achilles™ Satellite, resulting in an ICMP Monitor Failure.

To qualify for an exception, Wurldtech must accept that the exhibited behavior and the relevant design decision(s) are reasonable. The vendor must provide design documents that describe the device's behavior. Details of the exception to the pass/fail criteria will be made public, so the end user will be aware of the device's behavior. This practice is in line with Wurldtech's view that a key utility of certification is to ensure symmetric information between the customer and end user regarding a device's network robustness and resilience.

**Key Parameters for Level 1 Certification**

- Max link utilization: 10 percent.
- ICMP Monitor:
  - Timeout = 0.5 seconds.
  - Tolerable packet loss = 10 percent.
- TCP Ports Monitor:
  - TCP Ports: Use open ports from Discovery.
- UDP Ports Monitor:
  - UDP Ports: Use open ports from Discovery.
- OPC Monitor. A warning occurs if any of the following conditions are not satisfied:
  - System.Processes >= starting Number, where startingNumber is the number of processes active on the system during normal operation.
  - Processor(_Total).ProcessorTime < 100.
  - Process(_Total).WorkingSet < 125% of Starting Value, where Starting Value is the Working Set memory size during normal operation.
  - Process(_Total).PageFileBytes <125% of Starting Value, where Starting Value is the Page File memory size during normal operation.
- Linux System Monitor. A warning occurs if any of the following conditions are not satisfied:
  - CPU Usage (%) < 100.
  - Memory Usage < 125% of Starting Value, where Starting Value is the memory usage during normal operation.
  - Task Count >= Starting Number, where Starting Number is the number of tasks active on the system during normal operation.

## Test Cases and Parameters for Level 1 Certification

| Test Case | Test Type | Parameter Values |
|---|---|---|
| Ethernet Unicast Storm (L1) | Resource Exhaustion | Packet Length = 60, Rate Limit = 14880, Ethernet Protocol = IPV4, Duration = 120 |
| Ethernet Multicast Storm (L1) | Resource Exhaustion | Packet Length = 60, Rate Limit = 14880, Ethernet Protocol = IPV4, Duration = 120, Multicast IP Address = Use multicast IPs from discovery |
| Ethernet Broadcast Storm (L1) | Resource Exhaustion | Packet Length = 60, Rate Limit = 14880, Ethernet Protocol = IPV4, Duration = 120 |
| Ethernet Fuzzer (L1) | Invalid Packet | Number of Packets = 50000, Random Seed = Automatic, Source MAC Address = Local MAC, Destination MAC Address = Use DUT MAC |
| Ethernet Fuzzer (L1) | Invalid Packet | Number of Packets = 50000, Random Seed = Automatic, Source MAC Address = Local MAC, Destination MAC Address = Use multicast MACs from discovery |
| Ethernet Grammar (L1) | Invalid Packet | First Subtest = First in set, Last Subtest = Last in set |
| ARP Request Storm (L1) | Resource Exhaustion | Rate Limit =14880, Duration = 120 |
| ARP Host Reply Storm (L1) | Resource Exhaustion | Rate Limit =14880, Duration = 120 |
| ARP Cache Saturation Storm (L1) | Resource Exhaustion | Rate Limit =14880, Duration = 120, Random Seed = Automatic |
| ARP Grammar (L1) | Invalid Packet | First Subtest = First in set, Last Subtest = Last in set |
| IP Unicast Storm (L1) | Resource Exhaustion | Packet Length = 60, Rate Limit = 14880, Protocol = 17, Duration = 120 |
| IP Multicast Storm (L1) | Resource Exhaustion | Packet Length = 60, Rate Limit = 14880, Protocol = 17, Duration = 120, Multicast IP Address = Use multicast IPs from discovery |
| IP Broadcast Storm (L1) | Resource Exhaustion | Packet Length = 60, Rate Limit = 14880, Protocol = 17, Duration = 120, Broadcast IP Address = Local Network |
| IP Fragmented Storm (L1) | Resource Exhaustion | Rate Limit = 812, Duration = 120 |

| Test Case | Test Type | Parameter Values |
|---|---|---|
| IP Fuzzer (L1) | Invalid Packet | First Packet = 1, Last Packet = 50000, Random Seed = Automatic, Bad IP Version = 50, Odd IP Header Length = 50, Fragmented Packets = 50, Source IP Address = Random, Destination IP Address = Use DUT IP |
| IP Grammar - Field Fuzzer (L1) | Invalid Packet | First Subtest = First in set, Last Subtest = Last in set |
| IP Grammar - Fragmentation (L1) | Invalid Packet | First Subtest = First in set, Last Subtest = Last in set |
| IP Grammar - Options Fields (L1) | Invalid Packet | First Subtest = First in set, Last Subtest = Last in set |
| ICMP Storm (L1) | Resource Exhaustion | Packet Length = 60, Rate Limit = 14880, Duration = 120 |
| ICMP Grammar (L1) | Invalid Packet | First Subtest = First in set, Last Subtest = Last in set |
| ICMP Type/Code Cross Product (L1) | Invalid Packet | Packet Length = 60, Rate Limit = 14880, Protocol = 17, Duration = 120, Broadcast IP Address = Local Network |
| TCP Scan Robustness (L1) | Resource Exhaustion | Scan Mode =TCP SYN Scan, Destination TCP Ports = Use open ports from discovery, Use neighboring closed ports |
| TCP Scan Robustness (L1) | Resource Exhaustion | Scan Mode =TCP ACK Scan, Destination TCP Ports = Use open ports from discovery, Use neighboring closed ports |
| TCP Scan Robustness (L1) | Resource Exhaustion | Scan Mode =TCP FIN Scan, Destination TCP Ports = Use open ports from discovery, Use neighboring closed ports |
| TCP Scan Robustness (L1) | Resource Exhaustion | Scan Mode =TCP Connect Scan, Destination TCP Ports = Use open ports from discovery, Use neighboring closed ports |
| TCP Scan Robustness (L1) | Resource Exhaustion | Scan Mode =TCP Null Scan, Destination TCP Ports = Use open ports from discovery, Use neighboring closed ports |
| TCP Scan Robustness (L1) | Resource Exhaustion | Scan Mode =TCP XMAS Scan, Destination TCP Ports = Use open ports from discovery, Use neighboring closed ports |
| TCP SYN Storm (L1) | Resource Exhaustion | Rate Limit =14880, Duration = 120, Random Seed = Automatic, Destination TCP Ports = Use open ports from discovery, Use neighboring closed ports |
| TCP/IP LAND Attack (L1) | Resource Exhaustion | Rate Limit =14880, Duration = 120, Destination TCP Ports = Use open ports from discovery |
| TCP/IP LAND Attack (L1) | Resource Exhaustion | Rate Limit =14880, Duration = 120, Destination TCP Ports = Use open ports from discovery, Use neighboring closed ports |
| TCP Fuzzer (L1) | Invalid Packet | First Packet = 1, Last Packet = 50000, Random Seed = Automatic, Bad IP Version = 50, IP Options = 50, Fragmented Packets = 50, Bad TCP Checksum = 50, TCP Options = 50, Source TCP Port = Random, Source IP Address = Random, Destination TCP Port = First open port, Destination IP Address = Use DUT IP |
| TCP Grammar (L1) | Invalid Packet | Destination TCP Port = First open port, First Subtest = First in set, Last Subtest = Last in set |
| UDP Scan Robustness (L1) | Resource Exhaustion | Destination UDP Ports = Use open ports from discovery, Use neighboring closed ports |
| UDP Unicast Storm (L1) | Resource Exhaustion | Packet Length = 60, Rate Limit = 14880, Duration = 120 |
| UDP Multicast Storm (L1) | Resource Exhaustion | Packet Length = 60, Rate Limit = 14880, Duration = 120, Multicast IP Address = Use multicast IPs from discovery, Destination UDP Ports = Use open ports from discovery, Use neighboring closed ports |
| UDP Broadcast Storm (L1) | Resource Exhaustion | Packet Length = 60, Rate Limit = 14880, Duration = 120, Broadcast IP Address = Local Network, Destination UDP Ports = Use open ports from discovery, Use neighboring closed ports |
| UDP Fuzzer (L1) | Invalid Packet | First Packet = 1, Last Packet = 50000, Random Seed = Automatic, Bad IP Version = 50, IP Options = 50, Fragmented Packets = 50, Bad UDP Checksum = 50, Source UDP Port = Random, Source IP Address = Random, Destination UDP Port = First open port, Destination IP Address = Use DUT IP |
| UDP Grammar (L1) | Invalid Packet | Destination UDP Port = First open port, First Subtest = First in set, Last Subtest = Last in set |