achilles CERTIFICATION

Achilles Level 1 Certification Requirements for Embedded Devices

Embedded Device Definition

As proposed by ISA 99, an embedded device contains embedded software that directly monitors, controls, or actuates an industrial process. Examples include programmable logic controllers (PLCs), safety instrumented system (SIS) controllers and distributed control system (DCS) controllers.

Test Setup

The embedded device is programmed to produce a square wave output from its discrete output module. The square wave consists of an on period, where the output is high, followed by an off period, where the output is low. This cycle is to repeat indefinitely. While the device-under-test (DUT) is performing this operation, the Achilles™ Satellite executes the Achilles Level 1 Test Suite against the DUT and monitors its behavior.

Pass/Fail Criteria

Test results are determined by the Achilles Satellite's Discrete Monitor and ICMP Monitor. The status of each monitor must remain *Normal* during test execution, provided that the test case is executed on 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 a single test does not meet the aforementioned criteria, then the DUT fails Achilles Level 1 Certification.

Pass/Fail Criteria Exceptions

If the status of a monitor changes to *Warning* during test execution, an exception to the pass/fail criteria may be granted if the DUT's behavior is due to an explicit design decision. For example, suppose the DUT is designed to process up to 200 packets per second on a 100 Mbit link and ignore all traffic that exceeds this limit. Such behavior will likely result in the DUT not sending ICMP replies to the Achilles™ Satellite, resulting in an ICMP Monitor warning.

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.

Thus far, when granting pass/fail criteria exceptions, only ICMP Monitor *Warnings* have been exempted. ICMP Monitor *Failures* (the monitor status does not return to *Normal* by the end of the post-test period) and Discrete Monitor *Warnings* and *Failures* have not been exempted.

Key Parameters for Level 1 Certification

- Max link utilization: 10 percent.
- Discrete Monitor: Cycle period = 1000 milliseconds. Tolerable period error = 4 percent.
- ICMP Monitor: Timeout = 0.5 seconds. Tolerable packet loss = 10 percent.

Test Cases and Parameters for Level 1 Certification

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

Test Case	Parameter Values
IP Broadcast Storm (L1)	Packet Length = 60, Rate Limit = 14880, Protocol = 17, Duration = 120, Broadcast IP Address = Local Network
IP Fragmented Storm (L1)	Rate Limit = 812, Duration = 120
IP Fuzzer (L1)	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)	First Subtest = First in set, Last Subtest = Last in set
IP Grammar - Fragmentation (L1)	First Subtest = First in set, Last Subtest = Last in set
IP Grammar - Options Fields (L1)	First Subtest = First in set, Last Subtest = Last in set
ICMP Storm (L1)	Packet Length = 60, Rate Limit = 14880, Duration = 120
ICMP Grammar (L1)	First Subtest = First in set, Last Subtest = Last in set
ICMP Type/Code Cross Product (L1)	Packet Length = 60, Rate Limit = 14880, Protocol = 17, Duration = 120, Broadcast IP Address = Local Network
TCP Scan Robustness (L1)	Scan Mode =TCP SYN Scan, Destination TCP Ports = Use open ports from discovery, Use neighboring closed ports
TCP Scan Robustness (L1)	Scan Mode =TCP ACK Scan, Destination TCP Ports = Use open ports from discovery, Use neighboring closed ports
TCP Scan Robustness (L1)	Scan Mode =TCP FIN Scan, Destination TCP Ports = Use open ports from discovery, Use neighboring closed ports
TCP Scan Robustness (L1)	Scan Mode =TCP Connect Scan, Destination TCP Ports = Use open ports from discovery, Use neighboring closed ports
TCP Scan Robustness (L1)	Scan Mode =TCP Null Scan, Destination TCP Ports = Use open ports from discovery, Use neighboring closed ports
TCP Scan Robustness (L1)	Scan Mode =TCP XMAS Scan, Destination TCP Ports = Use open ports from discovery, Use neighboring closed ports
TCP SYN Storm (L1)	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)	Rate Limit =14880, Duration = 120, Destination TCP Ports = Use open ports from discovery
TCP/IP LAND Attack (L1)	Rate Limit =14880, Duration = 120, Destination TCP Ports = Use open ports from discovery, Use neighboring closed ports
TCP Fuzzer (L1)	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)	Destination TCP Port = First open port, First Subtest = First in set, Last Subtest = Last in set
UDP Scan Robustness (L1)	Destination UDP Ports = Use open ports from discovery, Use neighboring closed ports
UDP Unicast Storm (L1)	Packet Length = 60, Rate Limit = 14880, Duration = 120
UDP Multicast Storm (L1)	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)	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)	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)	Destination UDP Port = First open port, First Subtest = First in set, Last Subtest = Last in set