achilles CERTIFICATION
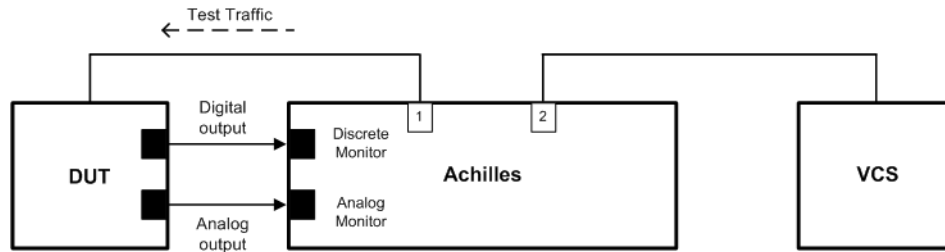
Embedded Device Definition

As proposed by ISA99, 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

Both digital and analog outputs are monitored by the Achilles®:

- The device under test (DUT) 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. The cycle lasts one second (500 msec high and 500 msec low) and repeats indefinitely.
- The DUT is programmed to produce an analog waveform that consists of 10 equal steps of increasing value and then 20 equal steps of decreasing value, both at one step per second, transitioning between the nominal minimum and maximum values of the output device.

While the DUT produces these two outputs, the Achilles executes the Achilles Level 2 test suite against the DUT and monitors its behavior. If the device only supports one of the two outputs, then only the existing output is monitored.

Pass/Fail Criteria

Achilles Monitors

Test results are determined by the following Achilles monitors:

- Discrete Monitor.
- Analog Monitor.
- Link State Monitor.
- ICMP Monitor.
- TCP Ports Monitor.
- UDP Ports Monitor.

Vendor-Defined Rate (VDR)

The Vendor-Defined Rate (VDR) is a packet rate that determines the certification criteria for a test. Tests run at or below the VDR have one set of criteria, whereas tests run above have another. The VDR is the rate at which one of the following two behaviors occur:

1 The device activates a rate-limiting mechanism that causes it to discard traffic.

2 The device drops packets as its performance limitations have been reached.

It is up to the vendor to specify the VDR and to provide documentation stating which of the above cases are occurring. In the case of the second behavior, it is possible the vendor will not know the VDR prior to testing. In this case, it may be specified after testing when the performance characteristics of the DUT have been determined. If the vendor chooses not to specify a VDR, then the stricter, "below-VDR" certification criteria is applied for all tests at all rates.

Required Monitor Behavior

- For every test run at or below the VDR:
  - The outcome of the Discrete Monitor, Analog Monitor, Link State Monitor, ICMP Monitor, TCP Ports Monitor, UDP Ports Monitor must be Normal.
- For every test run above the VDR, up to the full link rate or the maximum Achilles packet rate:
  - The outcome of the Discrete Monitor, the Analog Monitor, and the Link State Monitor must be Normal.
  - The outcome of the ICMP Monitor, TCP Ports Monitor, UDP Ports Monitor can be Normal or Warning.

Pass/Fail Criteria Exceptions

Exceptions to the above criteria may be granted if non-conforming DUT behavior is due to an explicit design decision or a device defense mechanism. For example, suppose a TCP service on the DUT only accepts x simultaneous connections. One of the Level 2 TCP tests results in more than x connections being made, leading to a TCP Ports Monitor warning as the monitor cannot create a new connection. Since the device is behaving as designed, the monitor warning is granted an exception.

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 DUT's behavior. The documented behavior is compared to the observed behavior, and if confirmed, the requested exceptions are granted. Details of the exception to the pass/fail criteria are included in the final certification report.

Key Parameters for Level 2 Certification

- Recovery period = 120 seconds
- Maximum Non-Storm Rate (% of Link) = Half the vendor-specified rate. Defaults to 5%.
- Discrete Monitor:
  - Cycle Period = 1000 milliseconds.
  - Warning Level = 4 percent.
- Analog Monitor:
  - Step Duration = 1.0 seconds.
  - Step Duration Error Tolerance = 4%.
  - Maximum Voltage and Minimum Voltage are DUT-dependent.
  - Voltage Error Tolerance = 1.0%.
- Link State Monitor: N/A.
- ICMP Monitor:
  - Timeout = 0.5 seconds.
  - Packet Loss Warning = 10 percent.
- TCP Ports Monitor:
  - TCP Ports = Use open ports from discovery.
- UDP Ports Monitor:
  - UDP Ports = Use open ports from discovery.