C54 An Audit-Based Architecture for Tribometric-Test-Data Verification

Mark I. Marpet, PhD, PE, St. John's University, 300 Howard Avenue, Staten Island, NY 10301*

After attending this presentation, attendees can expect to be familiar with the concept of audit-based test architecture and to understand how such an architecture can be implemented, using as an example Walkway Safety Tribometric-test (WST) equipment (devices to measure walkway friction).

The impact on the forensic community and/or humanity will be twofold: first, it will give the forensic community an awareness of issues in the legal community's acceptance of test data; secondly, it will suggest a method using multiple not-eraseable semiconductor memory to make test-data alteration far more difficult.

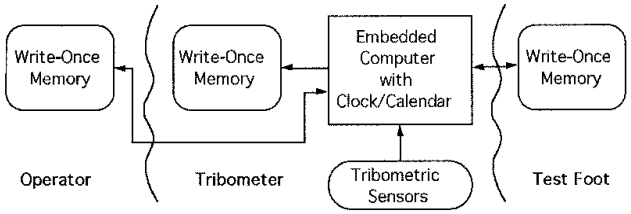
Test results are routinely challenged in the courtroom. Questions such as who conducted a test, when exactly was the test conducted, and so forth are routinely asked. On one level, this information is brought forth to lay an appropriate foundation, to show that the tests are legitimately conducted. On another, these questions are asked to root out inconsistencies, variations, or discrepancies, even trivial and inconsequential ones, that can be used to challenge the validity of the tests.

It cannot be ruled out that there exist a limited number of sophisticated and determined actors that can alter test data so that the detection of a test-result alteration becomes difficult or, perhaps, impossible to detect. Consequentially, no test result is ever completely beyond challenge. When the recording of test data is accomplished using a pad and pencil (or pen), as it is with most walkway-safety tribometers, test-result alteration is rather simple. On the other hand, it is possible, using both the standard 'paper-trail' concept and current technology, to make a test result very, *very* difficult to alter without detection. This paper discusses one approach to accomplish this, using multiple, write-once semiconductor memory devices in a manner that makes the cross-checking of the operator, instrument, test times, etc., with the test results, something essentially unalterable, which should greatly simplify the question of the provenance (factors relating to the origin) of the tests.

By way of background, a write-once memory device is an integrated circuit that, like an electronic odometer, has memory packets that cannot be rewritten once written to. In the same manner that an electronic odometer cannot be 'run backwards,' results recorded upon writeonce memory chips cannot be altered once written. By embedding serial numbers on each memory chip, it would be nearly impossible (which is not the same thing as impossible) to replace the memory chip with one having altered information.

The procedure for making a test system highly resistant to results tampering is to (a) identify each element in the system that is essential to system integrity, (b) supply each of those elements with a device having a write-once memory and, (c) have each of the identified elements of the test system communicate with the other elements at test time and mutually record the data and results in each of the write-once memory devices.

In WST testing, our example, the tribometer, the test technician, the test foot, and the date and time of day are essential elements of the testing. The tribometer would be fit with sensors that track test results (for example, many tribometers give results as a length or angle measurement, which is directly related to a slip-resistance value) and an embedded computer having clock/calendar and data-logging capabilities. The operator can be supplied and the test foot can be equipped with write-once data-loggers that are written to be the computer in the tribometer. Because the data-logging circuits for the operator and the test foot do not contain an embedded computer, they can be both small and inexpensive (the size and cost of a car-door remote control 'clicker'). Schematically, the arrangement is as follows:



The embedded computer creates, using a hashing or similar algorithm, a test code that will encapsulate the date, time, tribometer serial number, operator serial number, and test-foot serial number. That, along with the set of test results, is recorded in the three write-once memories. These memories can be printed out, providing a convenient test-record, and can be read by a properly equipped and programmed computer, providing an essentially unalterable snapshot of the information contained in the write-once memories. Some information, e.g., certification data for the operator, test instrument, or test foot, can be kept within the write-once memories for the operator, test instrument, or test foot respectively, and not written across the memories.

Obviously, this is a very flexible scheme, not restricted to tribometric instruments, and not restricted to the tribometer/ operator/test-foot combination described above. For example, this architecture could be implemented on blood-alcohol testing instruments, where the instrument, the operator, the calibration

 ** Presenting Author*

references, and the test results could all be concurrently written with the test results. In tribometric testing, temperature and relative humidity can be automatically recorded; more blue-sky-like, a compass circuit could give test direction, a GPS module could give approximate test location, and so forth, with the extent of test-parameter recording automation limited essentially by cost.

This architecture, because background and test-result data are automatically recorded on a number of not-necessarily co-located dataloggers, it makes inadvertent transcription errors impossible and the altering of already-written data essentially impossible. It is not, however, resistant to deliberate fraud. Two examples: (a) This described system is incapable of preventing a given operator from lending (or an unscrupulous person from temporarily 'borrowing') the operator's datalogger. Running with this, one could resort to fingerprint or retinal scan identification, to show that the operator is (at least) present, but cost would rise substantially if such measures had to be taken. (b) The clock/calendar could be deliberately mis-set in order to deceive. That is limited—like the entries in a laboratory journal—by the sequential nature of the not-rewriteable entries. To further prevent time/date tampering, the program that sets the date and time could be programmed to accept data only from a list of internet-based NTP time servers (http://www.ntp.org/), making it more than rather difficult to deliberately set an incorrect time.

Slip-and-Fall Accidents, Walkway-Safety Tribometry, Forensic Engineering

 ** Presenting Author*