Cybersecurity Risk Analysis Statement of SysMon II cards, and other EXELTECH Products

Following are standard operating procedures for the development, testing, storage, and delivery of any product capable of computation, and the delivery of Information technology and network accessibility.

1) All EXELTECH firmware is built in house, from source code, and controlled with secure PC's, firmware and source codes are kept together, and build revisions, date codes, and CRC checks are maintained.

2) No EXELTECH firmware is built with bootloading capability (no field upgrades), no patching, no firmware modification of any kind. Calibration values are not secured, they are controlled.

3) All EXELTECH firmware is protect with device read-only lockbits set during the programming process.

4) Firmware access control strictly enforced, all firmware is maintained in strict accordance to EXELTECH's TL9000 quality policy.

5) No generic default passwords or hidden administrator features exist. No capability to remote shutdown power systems exist.

6) All production software is deliverable, and no known testable vulnerabilities exist, no malicious code has ever been observed. No trivial process exists to circumvent our policies and rewrite or inject malware into our firmware process.