Requirements for Manufacturing and Test Equipment: TTM North America

The below are the requirements for TTM 4.0 Equipment which can be found at **on the TTM supplier's page at** www.ttm.com/en/suppliers.

1. *The machine must be capable of connecting to TTMs Industry 4.0 platform prior to leaving the factory over one of the following protocols:*
    a. *MODBUS*
    b. *OPC-UA*
    c. *MQTT*
    d. *Direct Communication through the following PLC drivers:*
        i. *Allen Bradley*
        ii. *Omron FINS TCP/UDP Must provide csv export of tag addresses in English*
        iii. *Omron NJ Driver Must provide csv export of tag addresses*
        iv. *Siemens S7-1500, S7-1200, S7-400, S7-300 Must provide tag addresses in English*

Others as approved by 4.0 team as long as they meet the data stream requirements.

2. *When machine is PC controlled, the connection will connect to the Ignition gateway as described above in #1.*
3. *Computers must be delivered with a current and supported operating system.*
    a. *Suppliers providing and supporting computers (embedded or free standing) will update operating system to current levels NLT 6 months prior to the end date for previous edition.*
4. *Computers containing operating systems shall be delivered up to date with patches.*
5. *Computers must be capable of accepting regular updates and patches.*
6. *Computers must be capable of running a TTM approved anti-virus/malware program.*
7. *Computers must be capable of joining Microsoft Active Directory and perform their intended function using an Active Directory service account.*
8. *Computers must be capable of industry standard data encryption in transit and at rest .*
    a. *At rest: FIPS validated Bitlocker or other TTM approved FIPS encryption methods*
    b. *In transit: IPSEC or other TTM approved encryption*
9. *Computers and software that handle sensitive data shall have the capability to log system and file access.*
10. *Vendor supplied software must be installed in a way as to not require administrative privileges for it to function properly.*
11. *Computers and software will be subject to vulnerability scanning; as a result of that, equipment should be resilient and not sensitive to scanning performed by TTM tools.*
12. *Equipment must have all unnecessary ports, protocols, and services disabled. Only necessary services shall be enabled unless necessary for the equipment to function properly.*
13. *Suppliers must be able to demonstrate robust controls for cybersecurity issues.*

Exceptions to above connectivity and security requirements will go through Engineering and IT Security.
The form to request exceptions can be found on the TTM supplier's page at www.ttm.com/en/suppliers. The form will be sent to the point of contact originating the request for quote.