

Semiconductor Equipment Security Challenges

Authors: Anant Raman, JB Ragothaman, Intel Corporation

Semiconductor equipment security is a multi-faceted challenge to IC Makers resulting from integrating embedded computing systems into the IC Maker Intranet. The integration poses three significant problems listed below:

- **Cyber security:** Embedded computers use modern day operating systems such as Windows and Linux expose the IC Maker factory networks to the risk of cyber-attacks causing significant business disruption and ensuing resource expenditure.

- **Intellectual Property (IP):** Prevailing software design of equipment do not clearly separate IC maker IP (process information) from Supplier IP (equipment information) leading to short term impacts on troubleshooting/problem solving and long term business impacts such as loss of trade secrets

- **System Integrity:** Current equipment designs have potentially serious operational impacts on uptime and performance. Anybody can walk up to equipment and with a click of a mouse can bring any equipment down impacting both IC makers and Suppliers financially

Cyber Security: Cyber security is a serious threat to the entire intranet including equipment. The pragmatic approach of "Network Isolate and Segment" versus "Patching" is working well as evidenced by no cyber infections in our factories. This approach takes the "full factory" and "functional area" perspectives for security related downtimes as an IC maker responsibility. We propose to extend the approach into equipment, hence impacting security-related downtimes additionally with focus at "equipment level". The blended approach also mitigates situations where IC makers are unable to provide their end of the "Network Isolate & Segment" method.

Intellectual Property: Clearly separating and controlling IC maker and Supplier proprietary information within equipment has been a long standing problem. Equipment software typically includes a stand alone application running on the equipment console with one login user running all the time in the foreground. The application is insensitive to the different roles in the factory – tool owners, field service engineers, manufacturing technicians, etc. The "one login" gives all users everybody's privileges highlighting the need of role based security and the impact of its absence – exposure of IP for both IC Makers and Suppliers. The paper will highlight critical IP areas in equipment for both IC makers and Suppliers and propose strategies to enable collaborative information sharing.

System Integrity: Described in the Intellectual Property section, the stand alone application running the equipment in the foreground, poses another problem. The User Interface (UI) and Application Logic (AL) are tightly integrated to the extent that bringing down the UI brings down the application, which in turn causes the equipment to go down. Bringing equipment down accidentally has significant impacts to the IC makers and suppliers. Application designs with decoupled UI and AL are essential to increased system integrity. Designing AL to run in the background further increases system integrity. .

The paper will propose a comprehensive security roadmap that highlights solutions for tactical issues such as cyber security and strategic long term issues such as system integrity and intellectual property. Cyber security, IP and System Integrity are targeted for the 2005 ITRS Roadmap.