

Empowering the semiconductor industry with advanced cybersecurity

End-to-end coverage

SEMICON Europa | November 2024

Agenda

Cybersecurity

1. HCLTech introduction
2. Challenges in semiconductor industry
3. Industry response to challenges
4. E187/E188 standards
5. Digital rights management
6. Application security
7. Cyber resilience act
8. IT security

No.1 India-headquartered company in TIME magazine's list of World's Best Companies 2024

Most decorated India-headquartered IT services company with No.1 rank in 21 categories in Technology IT Services & Software in 2024 Institutional Investor Research Asia Executive Team survey

Rated AA in the MSCI ESG ratings, A- by CDP for climate change actions and featured in S&P Sustainability Yearbook for two consecutive years

Ranked No.7 in India's Top 50 Most Sustainable Companies 2024 list by Businessworld

Named among 2024 World's Most Ethical Companies® by Ethisphere; ranked No.7 in India's Most Respected Companies 2024 list by Businessworld

HCLTech Founder Shiv Nadar named "India's most generous" for the third time in five years in Hurun Philanthropy List 2023

HCLTech Chairperson Roshni Nadar Malhotra conferred the Chevalier de la Légion d'Honneur, France's highest civilian award

Roshni Nadar Malhotra is the only Indian businessperson to be included in Fortune's list of 100 Most Powerful Women globally

HCLTech CEO & Managing Director C Vijayakumar honored with India's Best CEO Award in the IT Services – Super Large category by Fortune India

HCLTech at a glance

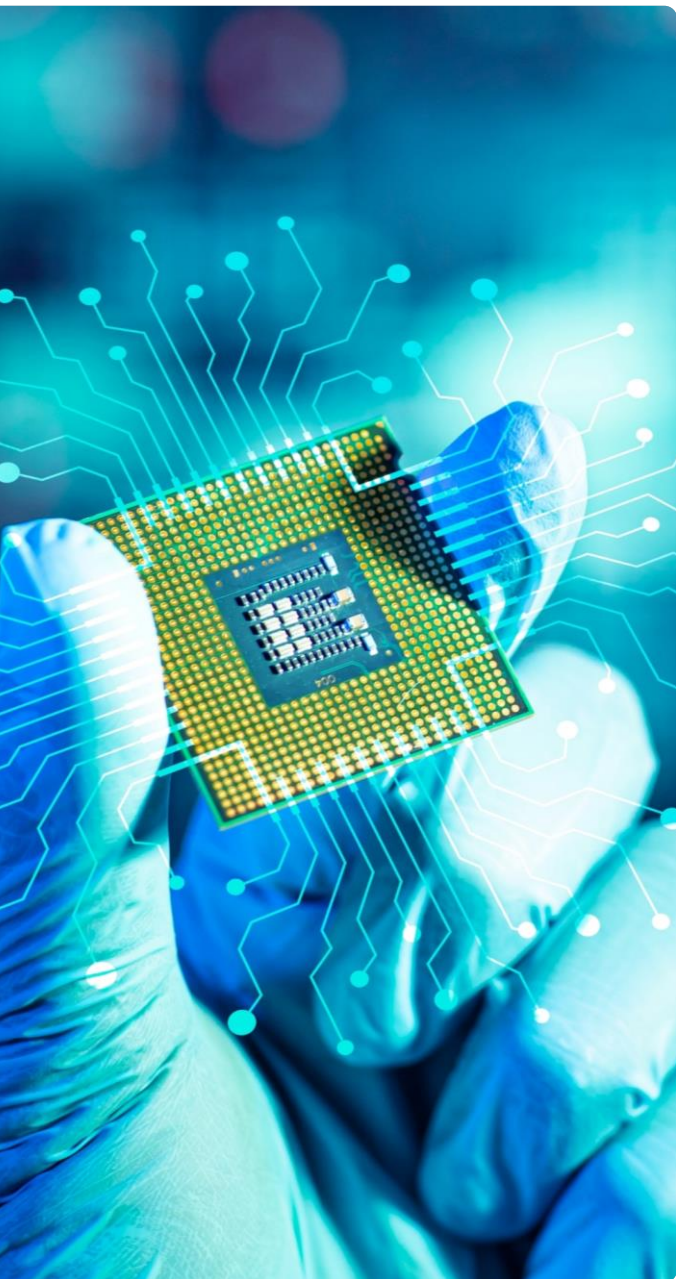


*For 12 months ending September 2024



Cybersecurity

Cybersecurity is essential in the **semiconductor industry** to protect intellectual property, sensitive designs, and manufacturing processes from cyber threats, which could lead to financial losses and compromised competitive advantage. Additionally, securing this critical infrastructure helps prevent potential disruptions in global supply chains and ensures the integrity of devices used in various industries.



Cybersecurity challenges in semiconductor industry

Fab and Equipment challenges

1 Intellectual property

The Fab environment hosts valuable IPs developed by foundries and chip design companies

2 Operational continuity

Disruptions often have a broader attack surface through cloud adoption, outdated SW, vulnerabilities and network connections

3 Safety of critical data

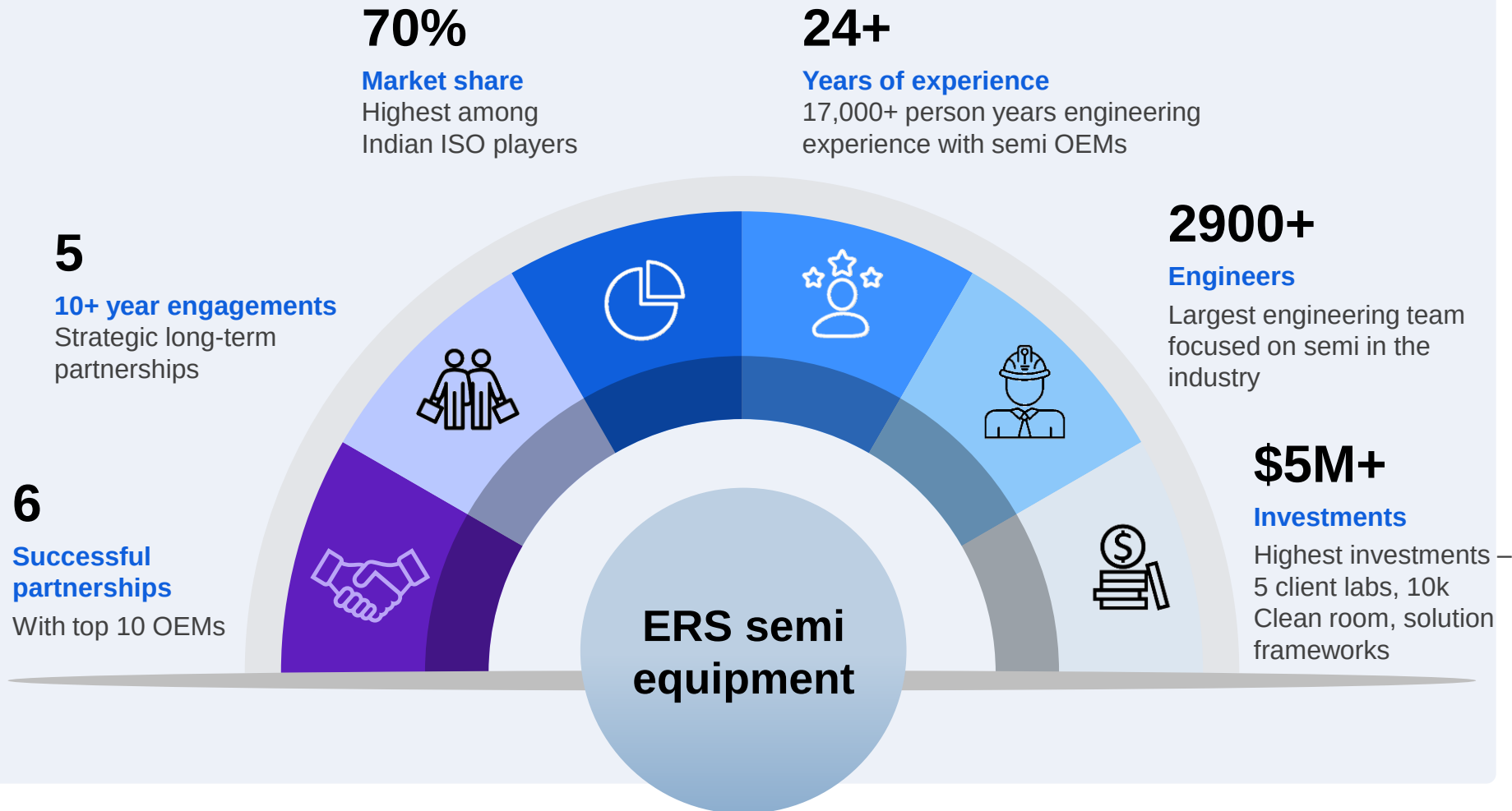
Equipment gathers and processes sensitive data during operation and production

4 Supply chain security

Semiconductor manufacturing relies on a global supply chain, partner cooperation and third-party integration

Vertical overview

ERS semi equipment – There's a bit of us in everything



HCLTech semi equipment lab

EFEM (Handler labs)

ATE labs

Mechanical and Electrical labs

Clean rooms

HCLTech 360 SecureOT- practice overview

Consulting and Advisory services

- OT-security program, Roadmap and Strategy consulting
- OT security site assessments, penetration testing
- IT-OT convergence cybersecurity strategy and architecture
- Third-party risk management
- Cybersecurity training, awareness and program management

Transformation and Managed services

- Connected things visibility (Inventory management and Threat intelligence)
- Zero trust architecture enablement (ZTNA, xDR, EPP, SRA, IGA, PAM, MFA, DLP, DAG)
- Managed protection services (OT systems, Network and data security technologies)
- OT device security (Pen-testing, application security and code review)
- Unified vulnerability management (Risk-based VA, PT, patching, patch governance)
- Security Incident detection and response (Anomaly detection, deception, analytics, SIEM/SOAR)



Customer centric engagements

- Globally present with local talent
- Adherence to local standards and compliances

Flexible delivery models

- Options of fully managed/co-managed/skill-on-tap
- Support customer tools or leverage HCLTech MSP platforms

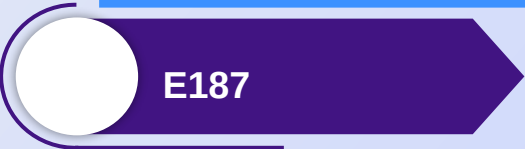
Transparent service offerings

- Pre-integrated as-a-service offers
- Modularity on service consumption and pricing

Industry approach to cybersecurity concerns

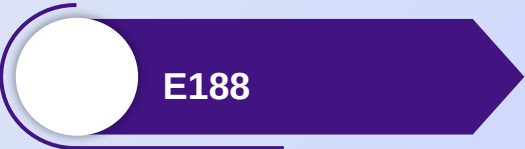
Equipment security

Latest Semi.org security standards



E187

Specification for cybersecurity of Fab equipment



E188

Specification for malware free equipment integration

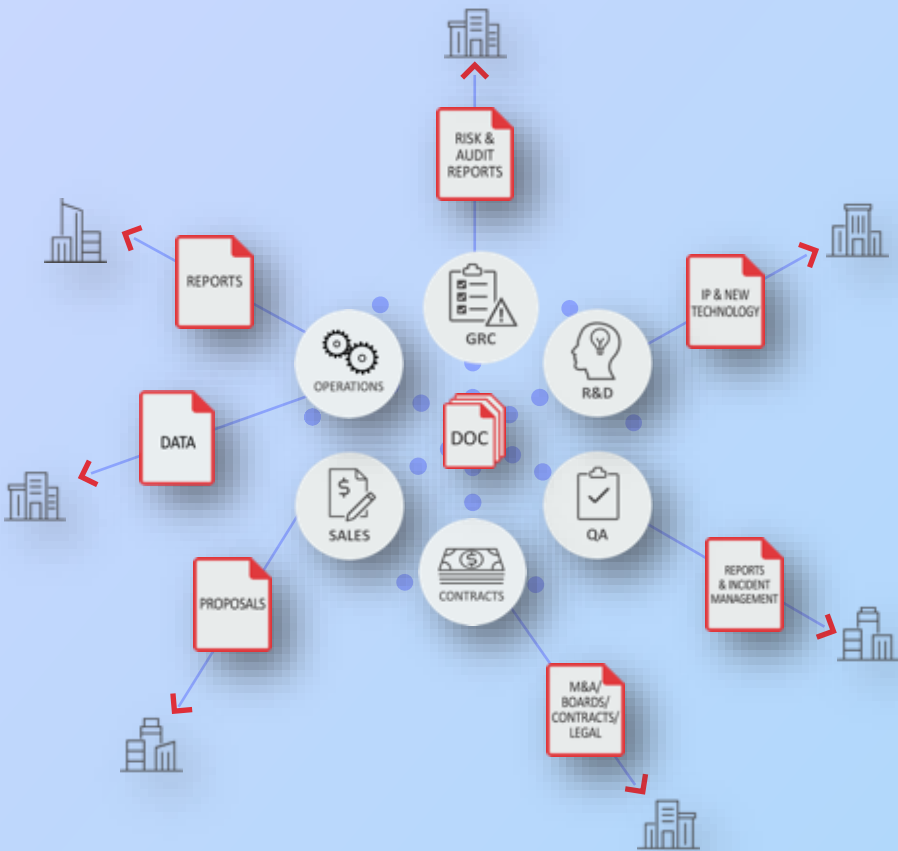
1
New security standards set by SEMI Fab and Equipment Information security task force led by **TSMC**

2
OEM's are striving to achieve E187 security compliance as a response to requests from Fab and OSAT

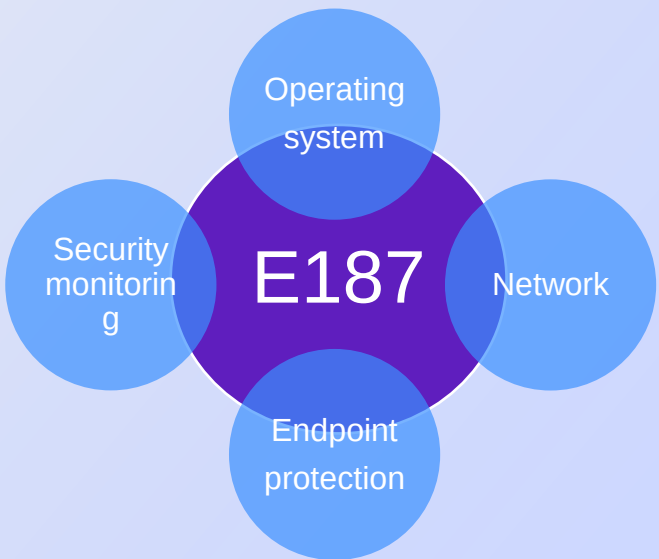
3
Applications migrated to cloud are assessed for vulnerabilities. DevSecOps with SAST, DAST and SCA is mandated with all application development

Data security

Digital Rights Management solutions for protecting OEM's IP/confidential information



Semiconductor equipment E187 compliance requirements



E187 – Compliance standard

OS hardening	440
Malware scan	1
Log monitor	80
Network hardening	140

Operating System (OS) support

- EOL
- OS security patch and updates
- OS hardening

Network security

- Network hardening
- Equipment applications – secure transmission protocols
- Documentation for network configuration/maintenance

Endpoint protection

- Vulnerability scan/Common Vulnerability Scoring System (CVSS)
- Malware scan
- Anti malware protection
- Documentation on security hardening
- Access control mechanism

Security monitoring

- Recording and exporting system and application logs
- System error, configuration changes and application security event logs

Assessment – priorities and scoring White paper at Semicon West

OS hardening rules	P1	P2	P3
Account policies	29	17	8
Security options	30	32	5
System services	10	11	3
Windows Firewall with advanced security	21	13	8
Advanced audit policy configuration	19	12	10
Administrative templates (computer)	15	12	9
Network	25	21	9
Event log service	24	19	5
Windows Defender antivirus (formerly Windows Defender)	9	5	4
Windows Defender exploit guard	4	16	2
Windows Remote Management (WinRM)	4	14	1
Administrative templates (user)	4	10	1
Total	194	182	65

Network security	P1	P2	P3
Network gate way	3	1	
Network security management	7	8	4
Harden network services	5	5	
Out of band management	4	3	2
Securing FTP and SFTP servers	7	8	2
Network configuration management	9	6	5
Network devices	4	6	2
Patch management	1	3	
Malware protection	4		
User account management	9	1	1
Email and Internet access	5	1	
IT policy	5	4	2
Security	9	3	2
Total	72	49	20

Equipment monitoring	P1	P2	P3
Certificate monitoring		4	1
Defense evasion	5		3
Log monitoring	3	3	3
Memory monitoring	1		
Network monitoring	2	3	2
Process monitoring	9	9	1
Script execution	7	2	1
Storage monitoring	2	1	
User access	10	2	3
Web monitoring	1	2	1
Total	40	26	15

The assessment rules could be prioritized based on equipment and environment

Appropriate weightage could be provided based on priority

The percentage of compliance could be calculated based on rules compliance and rules weightage

Secure collaboration for extended enterprises

Business need

Semi equipment organizations operate within a global supply chain, granting numerous individuals access to sensitive information. Controlled access to sensitive data is important.

Integrating Digital Rights Management solution into all systems (PLM/Enterprise Content management) that manage sensitive information allows companies to apply custom/granular access controls to documents independent of the type of document

Automatically grant access levels to users based on policies while they upload/download documents from repositories

Track and audit the actions performed by authorized users on the artifacts. Revoke document access from remote location if required.

HCLTech app security test methodology

Application security test methodology



Static analysis

- Secure code review is performed on the client specific application source code to uncover code level vulnerabilities



Dynamic analysis

- Vulnerability analysis and testing is conducted on runtime based on HTTP request and responses.
- Simulate the actions of actual attacker



Manual and automated penetration testing

- Exploit manually the vulnerabilities discovered in dynamic analysis
- Removal of false positives to confirm the authenticity of vulnerability



Vulnerability report analysis

- Expert analysis of the vulnerability reports
- Add remediation and recommendation techniques



Compliance determination

- Adhere to
 - PCI DSS
 - P II
 - HIPAA
 - FDA

Continuous security testing using various tools and HCLTech frameworks

CRA overview

European Cyber Resilience Act (CRA)

Proposal to strengthen cybersecurity rules for digital products

1

Addressing vulnerabilities and inconsistent provision of security updates

2

Many hardware /software products lack specific EU cybersecurity legislation

3

Cybersecurity services – CRA

#	Cybersecurity services for CRA	Details of the services	Applicable for semi equipment	HCLTech capability
1	Cybersecurity audits and assessment	Comprehensive security assessments of semiconductor manufacturing processes and ICS to identify vulnerabilities. Gap analysis to identify discrepancies between current practices and CRA requirements.	Yes	Yes
2	Vulnerability management services	Implement real-time vulnerability detection and reporting systems. Provide patches, updates, and mitigation strategies for known vulnerabilities.	Yes	Yes
3	Cybersecurity training and workshops	Specialized training for staff to understand and implement CRA requirements. Hands-on workshops to deal with cyber threats unique to semiconductor and ICS environments.	Yes	Yes
4	Incident response and forensics	Specialized incident response teams for quick mitigation of breaches or cyberattacks. Forensic analysis services post-incident to understand root causes and prevent future breaches.	Yes	Yes
5	Secure software/firmware development	Consulting on developing secure firmware and software for semiconductor devices and ICS. Regular updates to ensure security throughout the product's life cycle.	Yes	Yes
6	Consumer product security consulting	Even if they are considered non-critical, ensuring consumer products like monitoring tools or interface devices are secure and comply with CRA standards.	Yes	No

Cybersecurity services – CRA

#	Cybersecurity services for CRA	Details of the services	Applicable for Semi Equipment	HCLTech Capability
7	Integrated defense systems	Solutions that provide integrated protection across both physical (hardware) and logical (software) domains.	Yes (Integrated)	Yes
8	Secure connectivity and integration	Expertise in securely integrating ICS and semiconductor devices with broader networks, ensuring data integrity and security.	Yes (Integrated)	Yes
9	Cloud security solutions (if applicable)	With semiconductor and ICS data increasingly stored in the cloud, provide solutions that ensure cloud storage and processing meet CRA standards.	NA	Yes
10	Regulatory compliance assistance	Regular updates on CRA amendments and requirements. Assistance in ensuring continuous compliance with evolving standards. Facilitate certification and documentation processes.	Yes	No
11	Network security solutions	Securing interfaces and network connections in semiconductor and ICS environments. Implementing encryption, secure authentication methods, and intrusion detection systems.	Partial	Yes
12	Supply chain security management	Develop protocols and systems to ensure cybersecurity standards are maintained across the supply chain. Vetting and evaluation of third-party suppliers/vendors to ensure they meet CRA standards.	Yes	Partial
13	Secure product development consulting	Expertise in designing semiconductor products and ICS components that adhere to the cybersecurity standards set by the CRA. Lifecycle management, ensuring semiconductor products remain secure from conception through decommissioning.	NA	No

Visit us at Hall C2 booth 808

HCLTech at SEMICON Europa 2024



HCLTech | Supercharging
Progress™

hcltech.com