The Future of Trusted Computing

Steve Hanna
Co-Chair, Embedded Systems Work Group, TCG
Senior Principal, Infineon Technologies

Agenda

- TCG Vision
- Today’s Reality
- Securing IoT and Cloud
- Conclusion
- Questions and Discussion

TCG VISION

TCG Vision

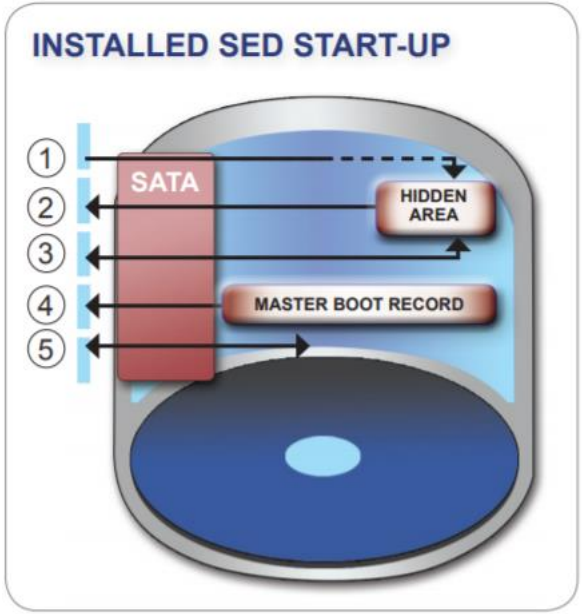
"TCG Enabled" internationally standardized technology is *globally accepted and expected as the foundation for trust* in systems ranging from the most complex large-scale computing platforms to small scale dedicated devices, from traditional IT to the factory floor to the myriad devices which enrich our daily lives

“TCG-Enabled” Technology

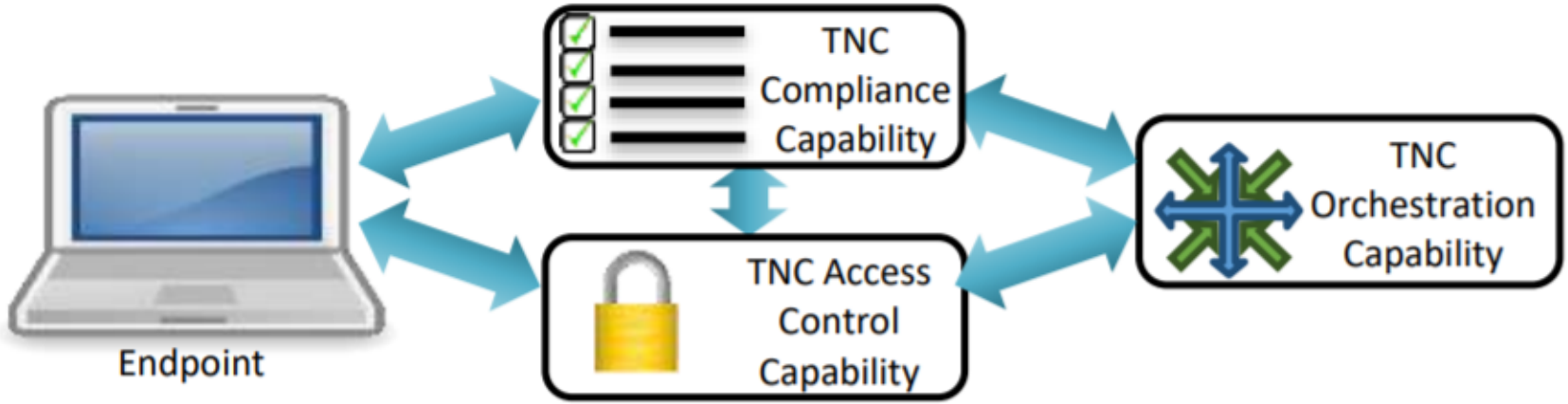
- TPM (Trusted Platform Module)
- DICE (Device Identifier Composition Engine)
- SED (Self-Encrypting Drives)
- TNC (Trusted Network Communications)

SED Overview

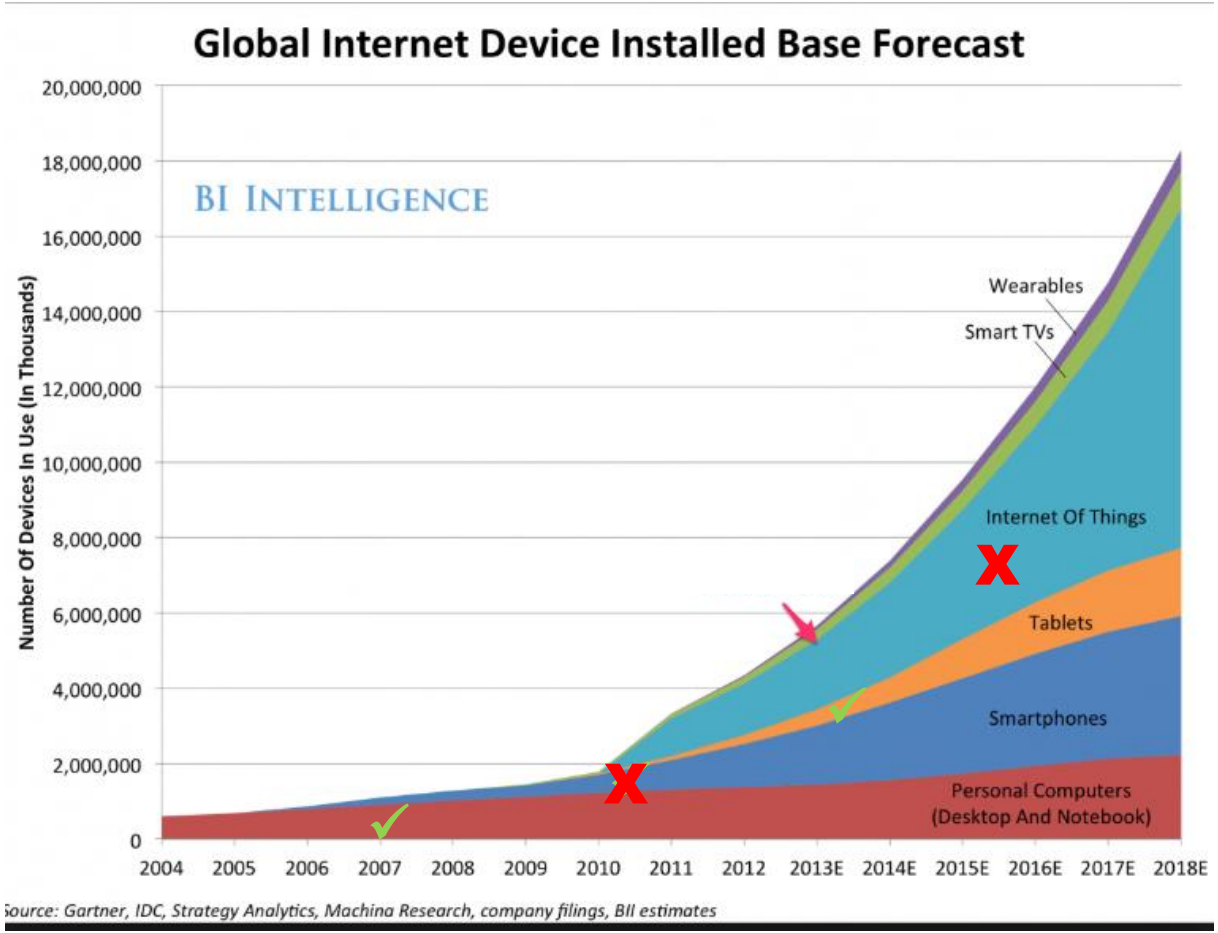
1. Initial Boot
2. Pre-Boot OS
3. User Authentication
4. Boot into Normal OS
5. Normal operation, with inline hardware encryption



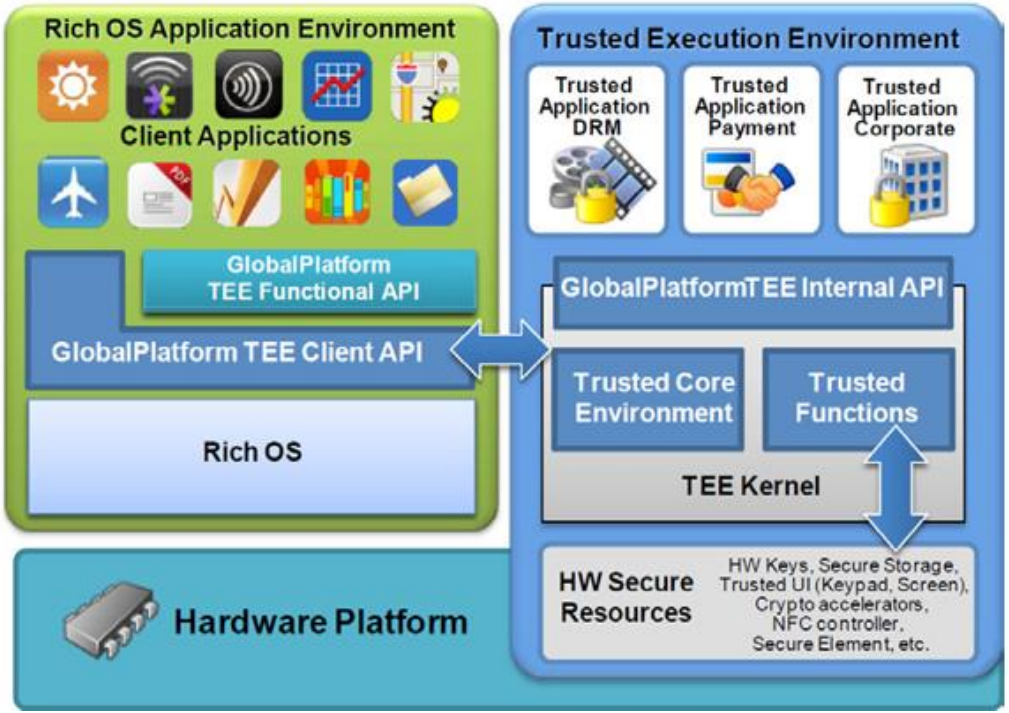
TNC Overview



TODAY’S REALITY



TEE – Trusted Execution Environment



Graphics Source: UL; White paper - HCE security implications, analyzing the security aspects of HCE (Jan 8, 2014)

IoT Attacks Growing

SECURING IOT AND CLOUD

IoT Defined

"A world where **physical objects** are seamlessly **integrated** into the **information network**."

Why IoT?

Automotive	Smart Home	Industrial	ICT
			

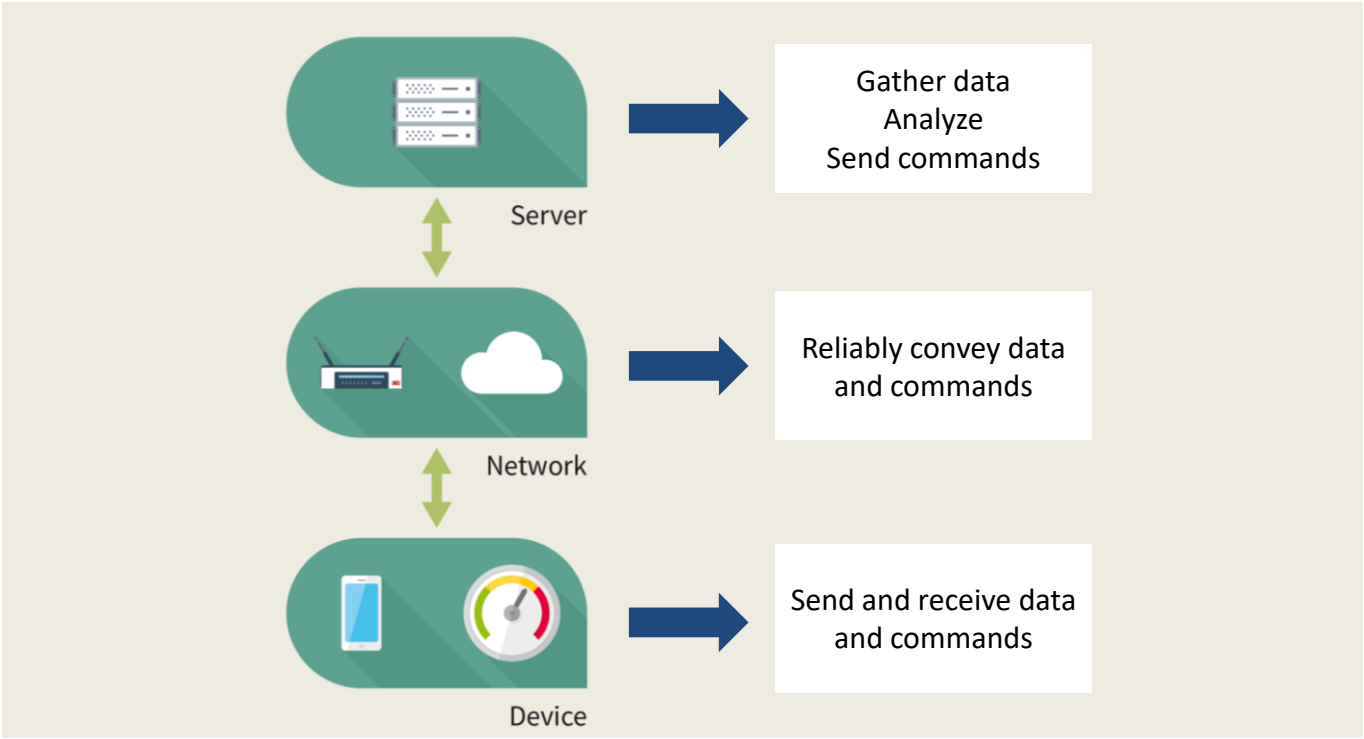
1	New capabilities and services
2	Greater efficiency
3	Increased flexibility and customization

IoT Affects Everything

Smart Vehicles	Smart Cities & Energy	Smart Industry & Business	Smart Home & Consumer Devices
Smart Cars	Energy	Factory Automation	Smart Home
Commercial, Agri-culture & Construc-tion Vehicles incl. Trucks & Busses	Building Automation	Medical Equipment	Smartphones, Tablets & PCs
Low speed vehicles	Professional Lighting	Other Business	Consumer Electronics & Wearables
Other Transport	Infrastructure		

Smart ICT	
Communication Networks	Data Center / Cloud

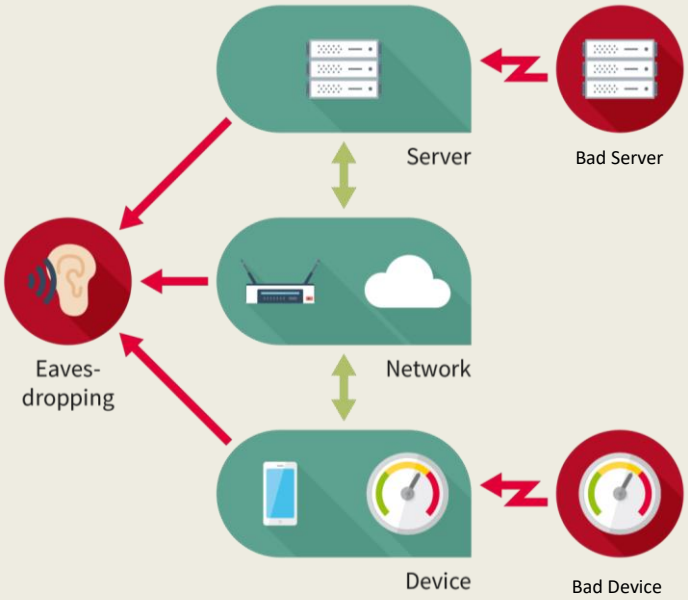
IoT Architecture



Each layer can be attacked

Security threats for IoT

An **Eavesdropper** listening in on data or commands can reveal confidential information about the operation of the infrastructure.



A **Bad Server** sending incorrect commands can be used to trigger unplanned events, to send some physical resource (water, oil, electricity, etc.) to an unplanned destina-tion, and so forth.

A **Bad Device** injecting fake measurements can disrupt the control processes and cause them to react inappropriately or dangerously, or can be used to mask physical attacks.

Top challenges for IoT adopters

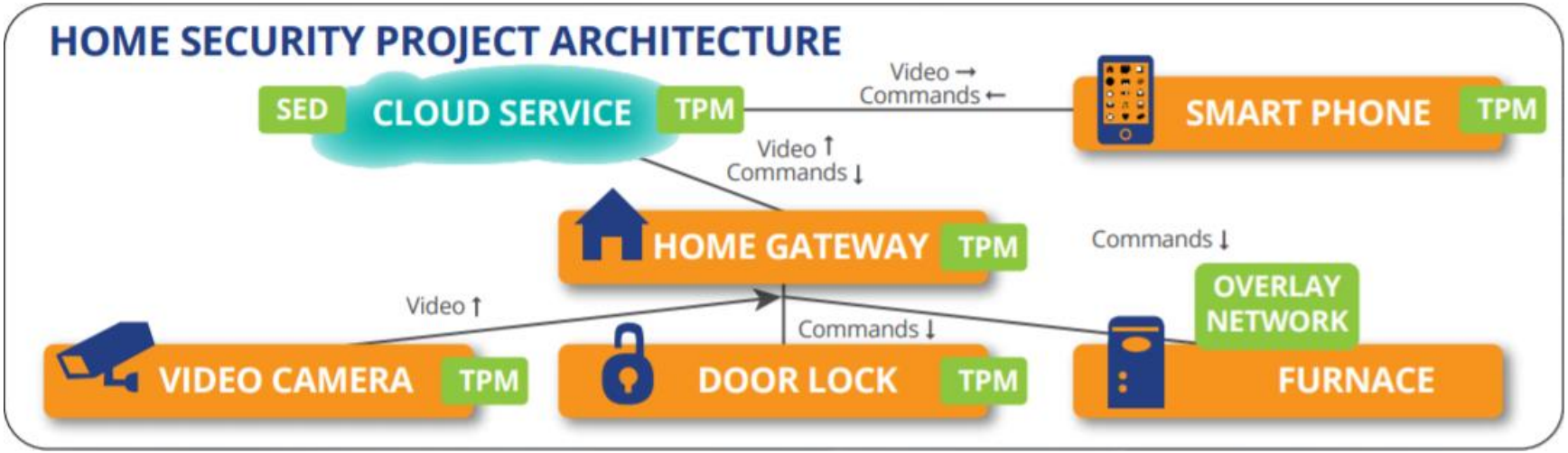
1. **Cybersecurity**
2. **Integration**
3. **Managing business requirements**

Source: Gartner survey results, March 3, 2016
http://www.gartner.com/newsroom/id/3236718

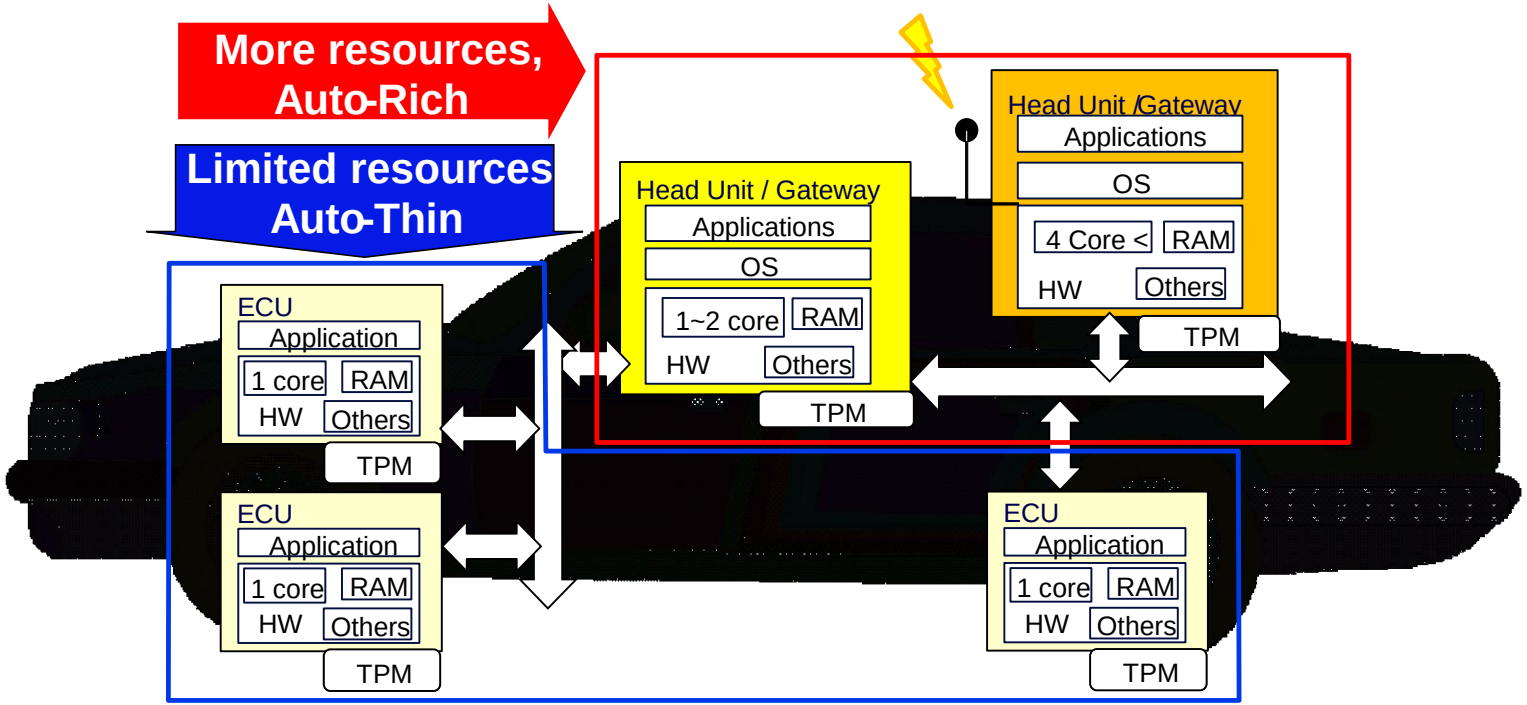
TCG Work on Securing IoT

- Published
  - TCG Guidance for Securing IoT
  - Automotive-Thin Profile for TPM
  - DICE Architectures
- In Progress
  - TCG Guidance for Securing Industrial Systems
  - Cyber Resilient Technologies

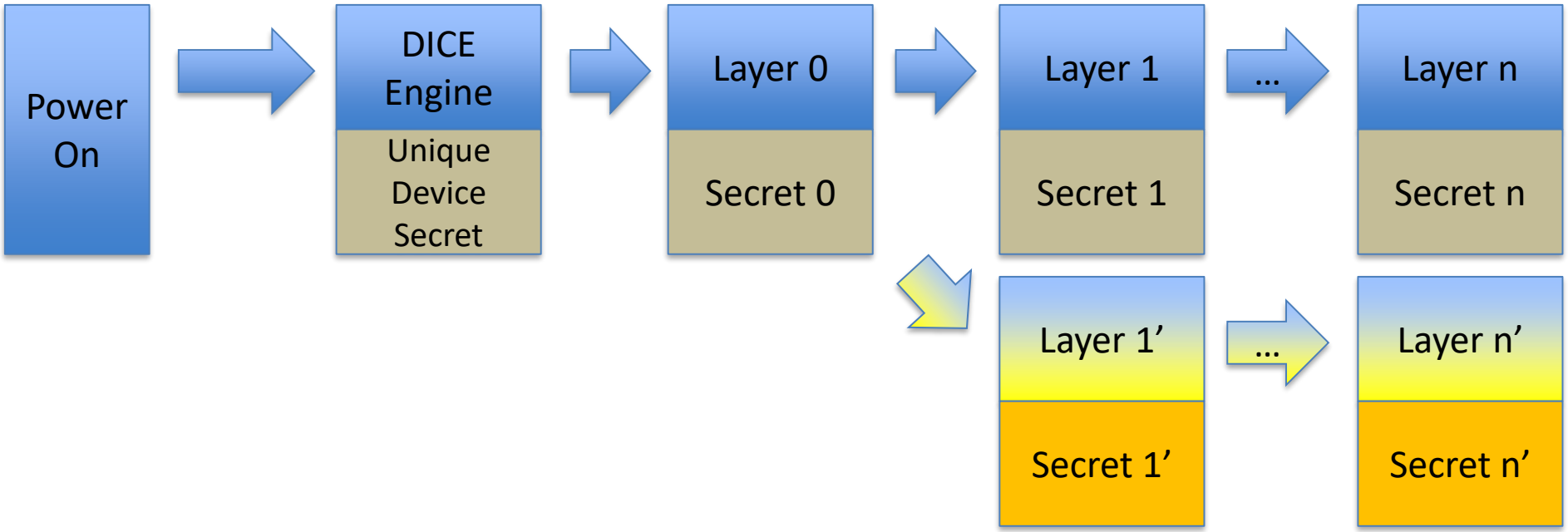
TCG Guidance for Securing IoT



Automotive-Thin Profile for TPM

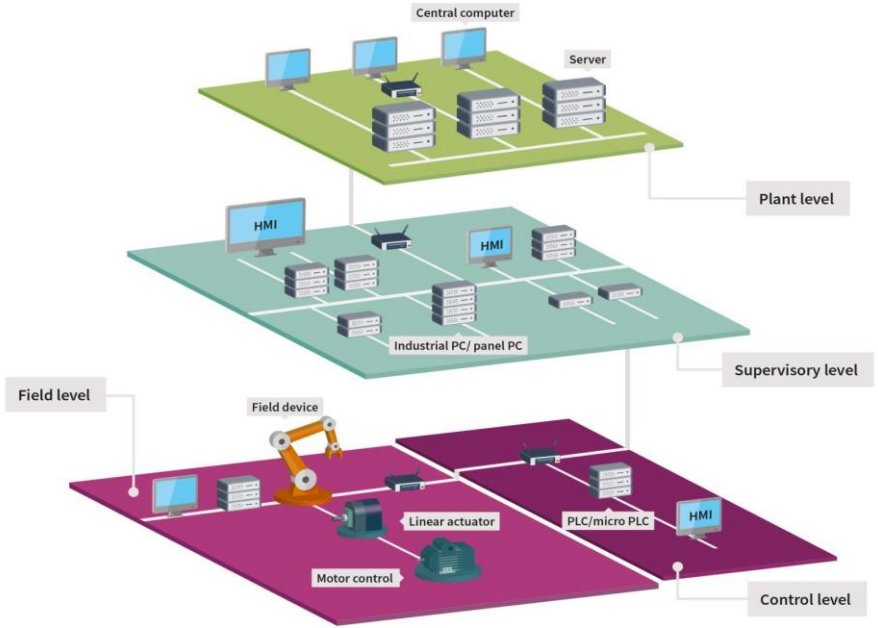


DICE Architectures



Work in Progress

TCG Guidance for Securing Industrial Systems



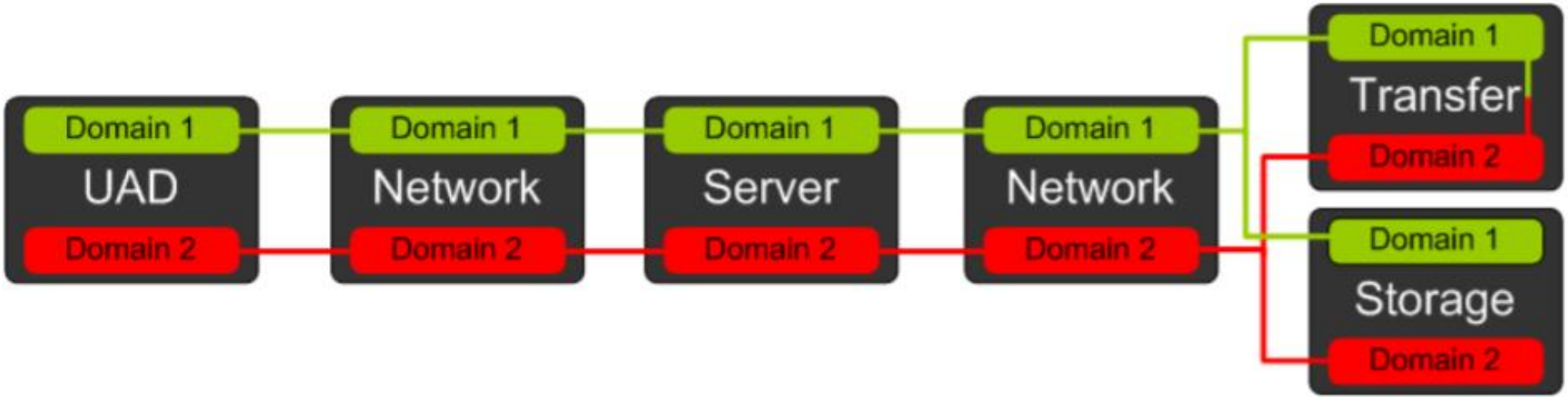
Cyber Resilient Technologies

- **Protect** updatable persistent code and configuration data
- **Detect** when vulnerabilities are not patched or when corruption has occurred
- **Recover** reliably to a known good state even if the platform is compromised

TCG Work on Securing Cloud

- Published
  - Trusted Multi-Tenant Infrastructure Trust Assessment Framework
  - Trusted Multi-Tenant Infrastructure Use Cases
  - Trusted Multi-Tenant Infrastructure Reference Framework

Trusted Multi-Tenant Infrastructure



CONCLUSION

What Lies Ahead?

- New applications for Trusted Computing
- New challenges and threats
- New ideas for addressing those threats

QUESTIONS AND DISCUSSION