Empowered by Innovation NEC

Issues in Secure DV-LSI Design

（セキュアなDV-LSI設計での諸課題）

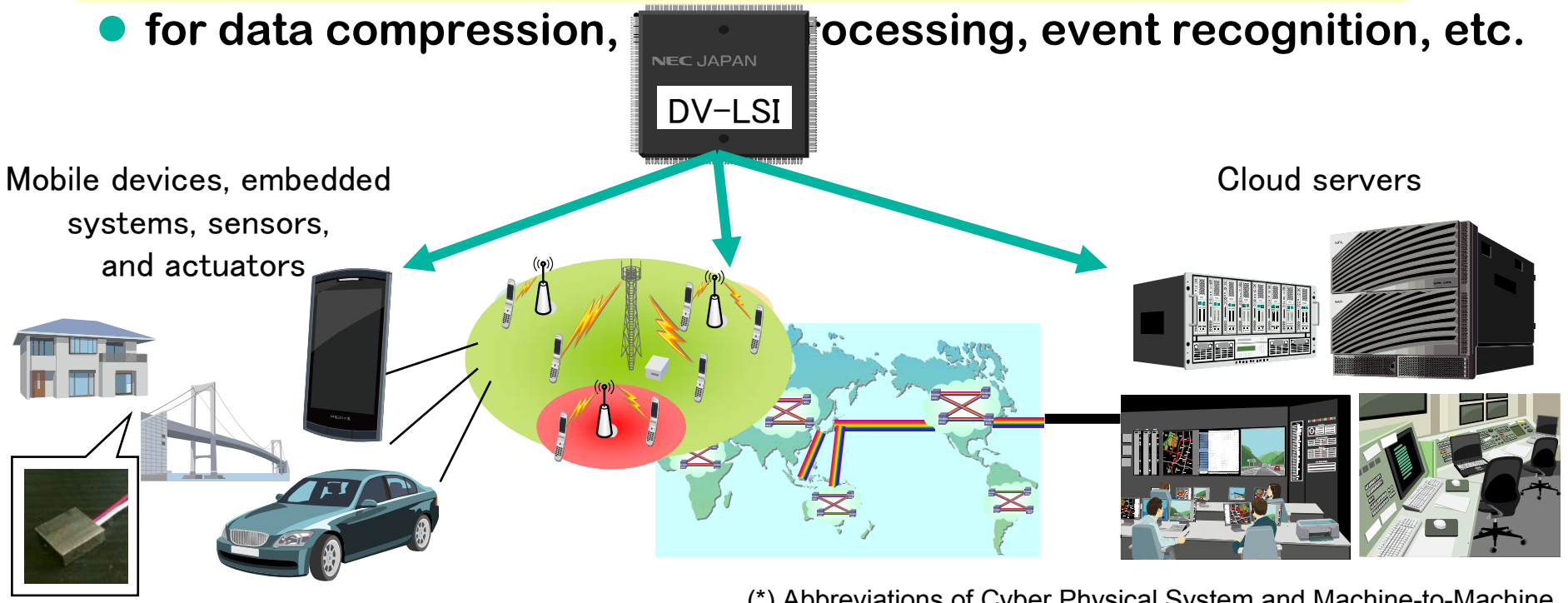
June 8, 2012
Sumio Morioka（s-morioka@ak.jp.nec.com）
Central Research Laboratories, NEC Corporation

DV-LSI research in fabless ICT companies

Main targets of our R&D: *CPS*, M2M*, sensing and actuation*.

DV-LSIs will be key devices:

- for real-time data processing and low power (green of ICT).
- for data compression, [illegible]ocessing, event recognition, etc.



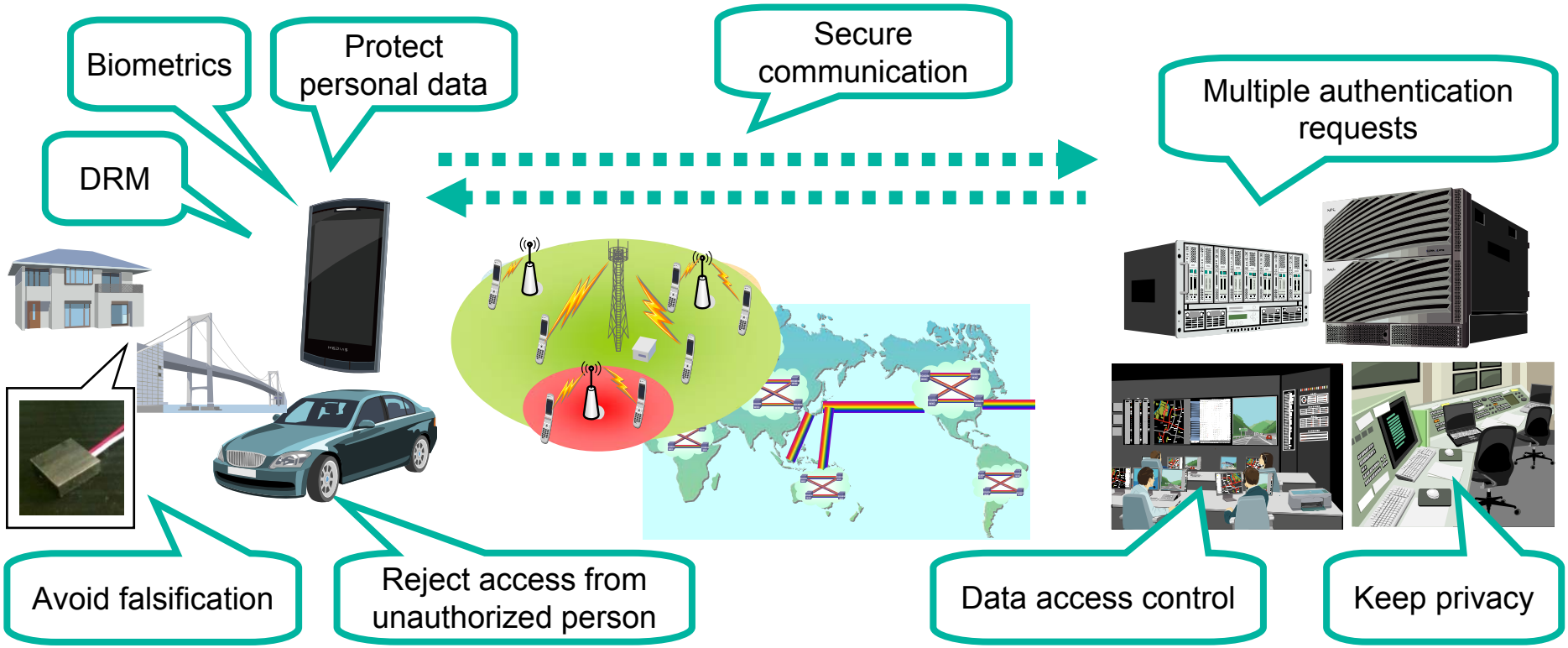
(*) Abbreviations of Cyber Physical System and Machine-to-Machine.

Copyright © 2012 NEC Corporation

Demands for stronger security in future ICT

DV-LSIs will be widely used:

- to accelerate complicated security computations.
- to achieve high tamper resistance.



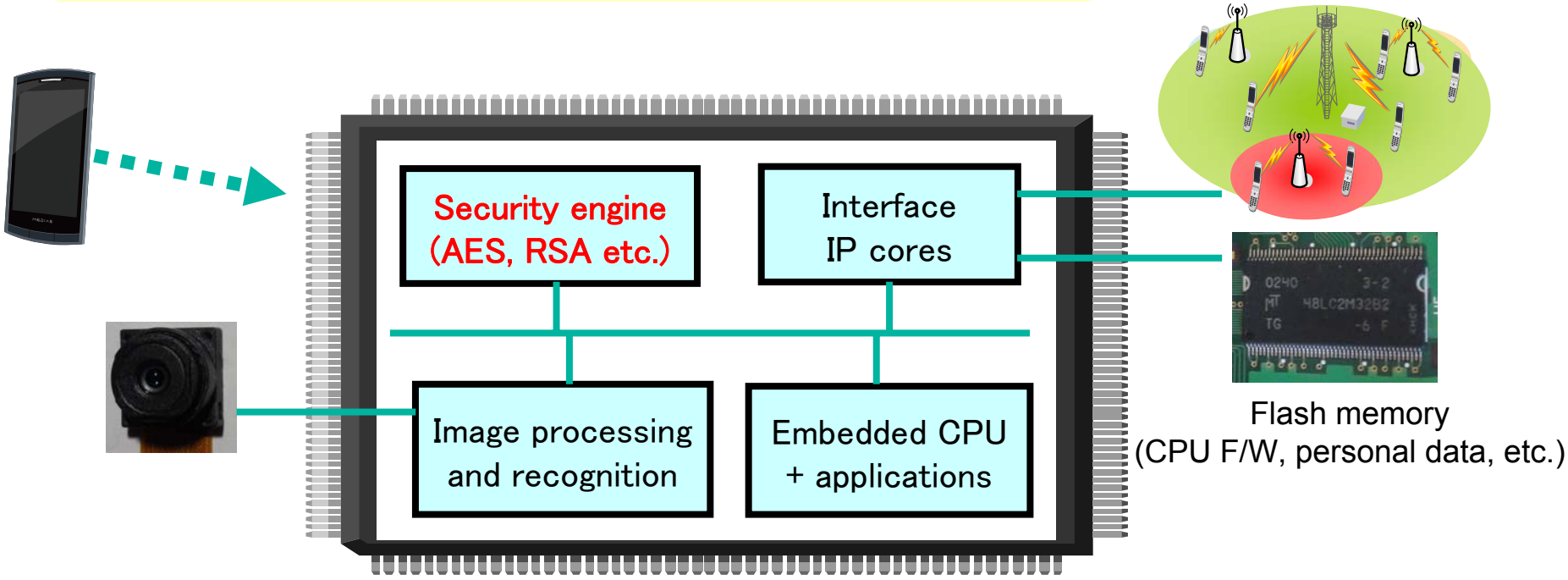
Copyright © 2012 NEC Corporation

Single LSI handles multiple security functions

Not only cryptography, but key exchange, authentication, secure protocol, biometrics, … are integrated.

Most LSI designers…

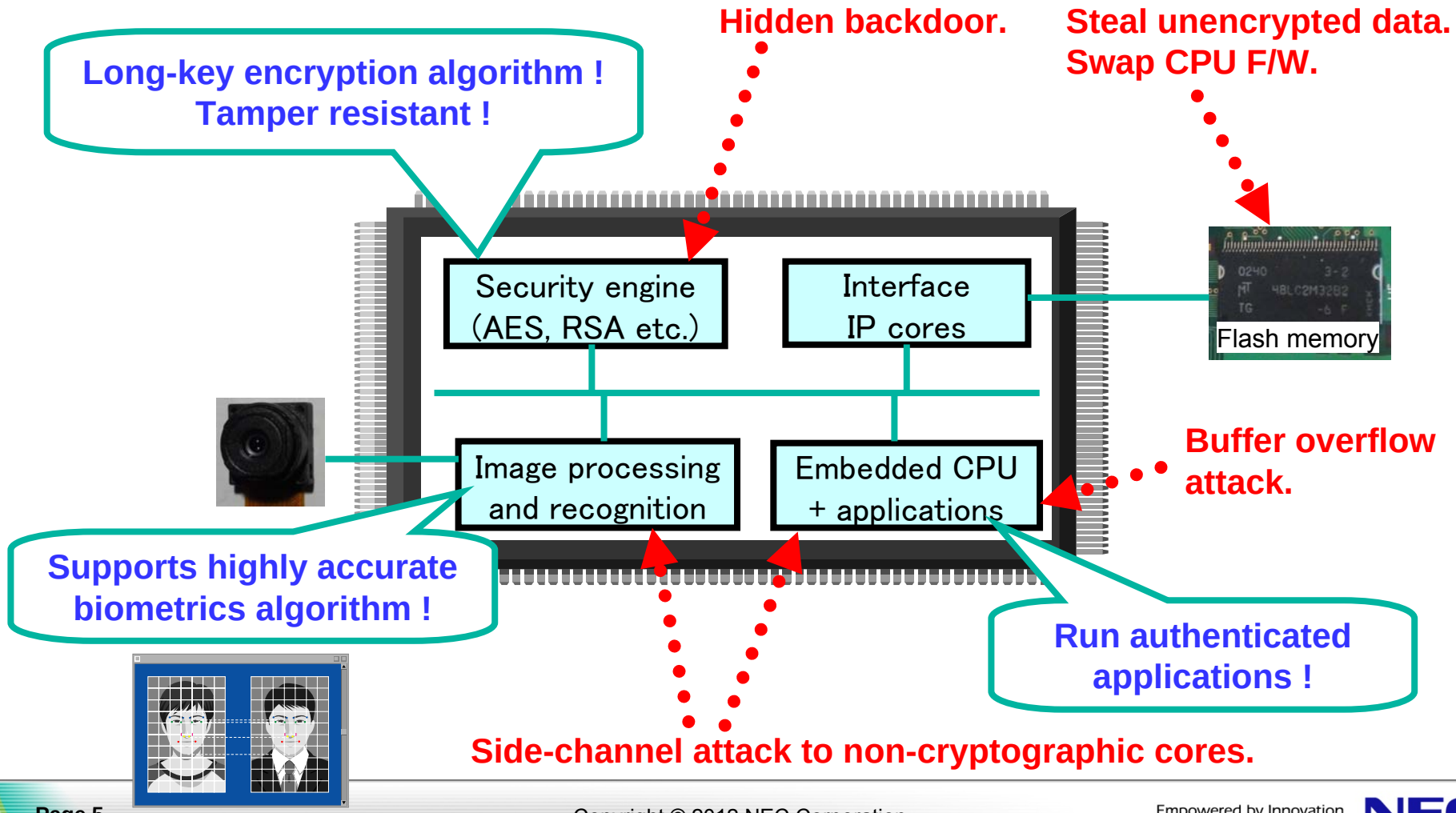
- consider attaching cryptographic IP is sufficient.
- don't verify *if total system is secure*.



Copyright © 2012 NEC Corporation

Issue 1: Total security ≠ Σ partial security

Collection of countermeasures to attacks does *not* mean there is no security hole.



Copyright © 2012 NEC Corporation

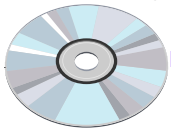
Issue 2: Over specification of security cores

IP-core researchers try to achieve very strong security

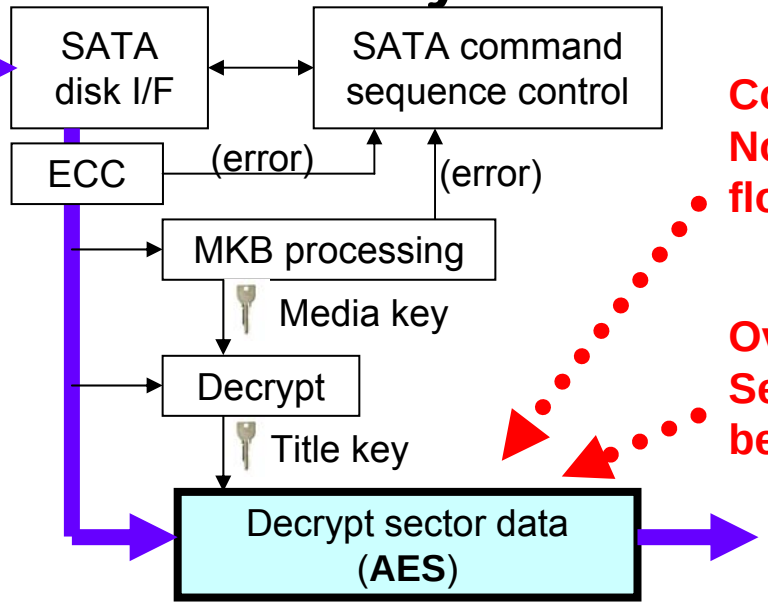
DPA resistant AES
- custom-made process library
- asynchronous design

Secret key does not leak out even if 1M waveforms are used !

Over specification and too costly in some systems.



Optical Disk
(DRM: AACS)



Costly:
Non-standard design flow and process.

Over spec.:
Secret key is different between disk sectors.

Copyright © 2012 NEC Corporation

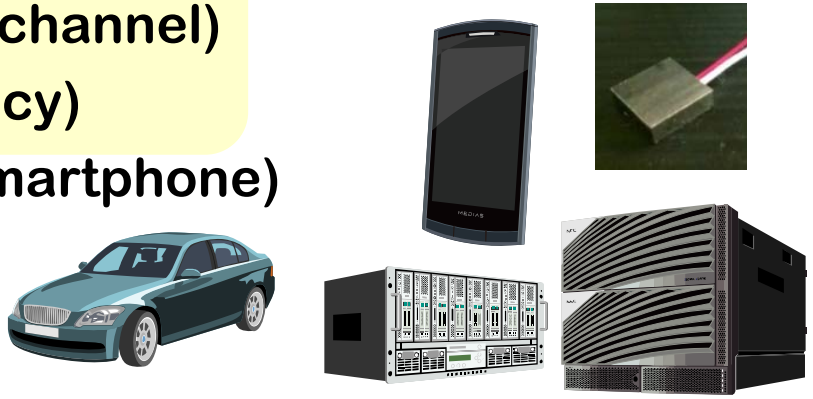
Issue 3: Rapid change of security requirements

Existing implementation standards: NIST FIPS 140-2/140-3, ISO/IEC 19790:2006, 24759:2008, etc.

- Security requirements for cryptographic modules.
- Involving side-channel attacks is *still* under discussion.

Security standards are necessary, yet insufficient against…

- new kinds of attacks. (ex. side-channel)
- new security concepts. (ex. privacy)
- new commercial products. (ex. smartphone)



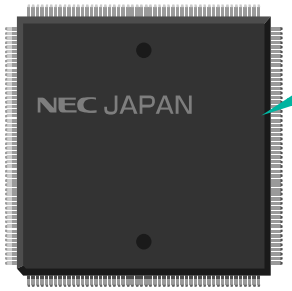
Copyright © 2012 NEC Corporation

Other important issues

Recent trends of LSI development.

- Fabless companies.
- Expanding use of FPGAs.
- Expanding use of ESL/HLS environment.

How to upgrade security functions after release to the market?



Lifetime of LSIs in social infrastructure can be very long. (5～20 years?)

New attack methods will be developed…

Copyright © 2012 NEC Corporation

Important directions of “secure” DV-LSI research

How to achieve *total security* of *system LSIs*? (H/W + S/W)

- Design and verification methodology for finding security holes.
- Special support by EDA tools.
- Design team organization and management.

How to optimize overhead costs of security mechanism?

- Implement over multiple design layers and/or components.

Device independent security H/W.

Flexible yet secure LSI.

Reference: Sumio Morioka, ″The Inevitable Use of Behavioral Synthesis in Advanced Security Hardware Designs,″ TUTORIAL 2: High-Level Synthesis for ESL Design: Fundamentals and Case Studies, The 46th Design Automation Conference (DAC), 2009.

Copyright © 2012 NEC Corporation