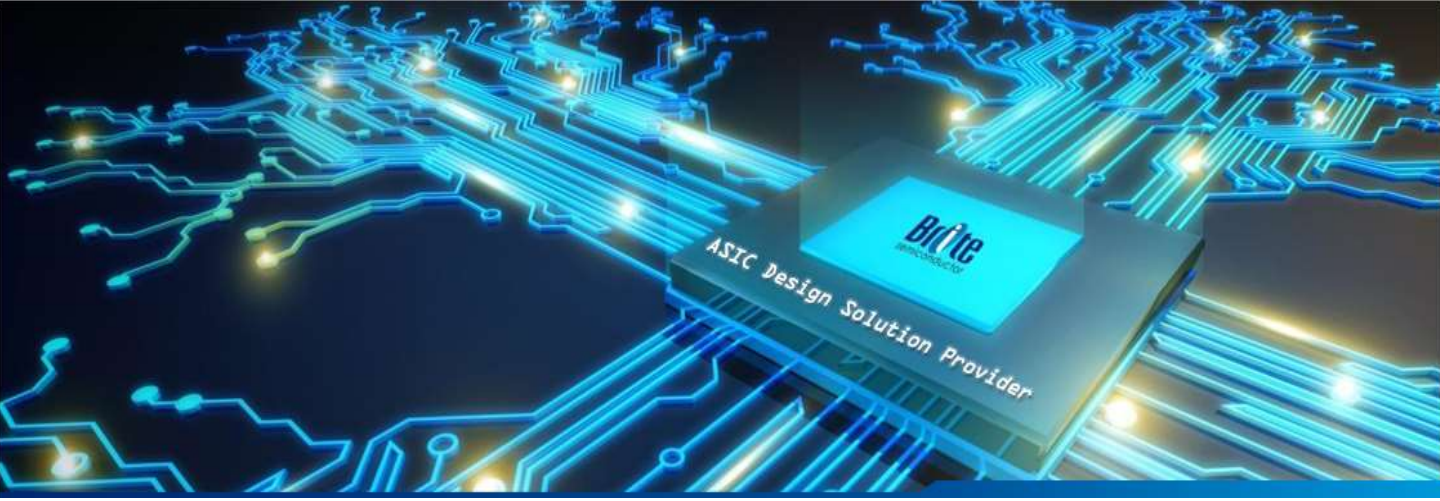


Security Solution In ASIC Design At Front-end And Back-end Phase

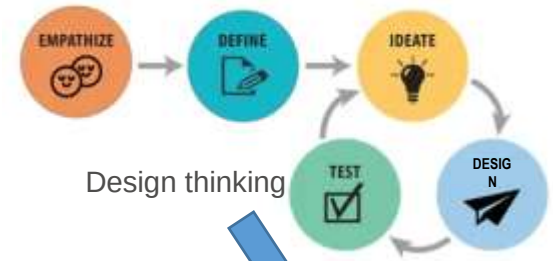
Yadong Liu

2021.3.18

Brite semiconductor

Design For Security

Design for Security can be seen as Design Thinking applied to Security



Security

Design for Security

BEFORE THE DESIGN

* Identification of goods
* Threats
* Protections
* Mapping
* Development plan

DURING THE DESIGN

* Specifications Review
* Code Review
* Analysis of Threats
* Quotation of Attacks

AFTER THE DESIGN

* Test Plan
* Assistance to Certification
* Help for Documentation
* Design of Patches

Adapt Your Defenses To Usages And Opponents

The security needs of the device must be defined with usage and potential threats in mind.

First step is therefore to determine the assets, then the threats and finally all the potential points that may be exposed to an attack (the vulnerabilities)

Each device has its own characteristics and functionalities. Therefore, those definitions are different from one device to another.

- **The considered assets to protect:**
  - Input data
  - Output data
  - Intellectual property
  - Computational power
  - Functionality/Availability
  - User's life…
- **Time in lifecycle**
  - In the factory
  - In the field
  - After decommissioning
- **The potential threats**
  - Cyber threats on the device
  - Cyber threats on the service/platform
  - Physical threats on the device…
- **The potential attackers**
  - Their means
  - Their motivations (lucrative, idealistic, revenge, …)

Probably good against knights…
Certainly useless against hackers
Not very handy for a Smartphone!

The security need is the combination of assets, threats and weaknesses.
This definition of the security need is the basis of the design for security.

Threat Analysis Risk Assessment (Tara) Approach

Once Security needs have been assessed, they must be rated and addressed

Define assets and associated security attributes (confidentiality, integrity, availability, etc.)

Define the damage potential

Define the possible Threats and their risk factor (time, access, knowledge, equipment)

Calculate Risk level (using risk factor and damage potential)

Define countermeasure(s) associated to vulnerabilities


ISO IEC

ISO/IEC JTC 1/SC 27/WG 3 **N1652**

REPLACES:

ISO/IEC JTC 1/SC 27/WG 3

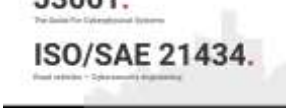
Information technology - Security techniques - Security evaluation, testing and specification

Convenorship: AENOR, Spain, Vice-convenorship: JISC, Japan

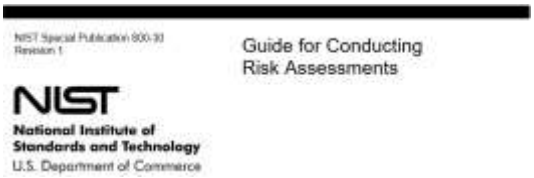
DOC TYPE: working draft

TITLE: CD Text for ISO SAE 21434 — Road vehicles — Cybersecurity engineering

SOURCE: ISO TC 22/SC 32/WG 11


J3061.

ISO/SAE 21434.


NIST Special Publication 800-30 Revision 1

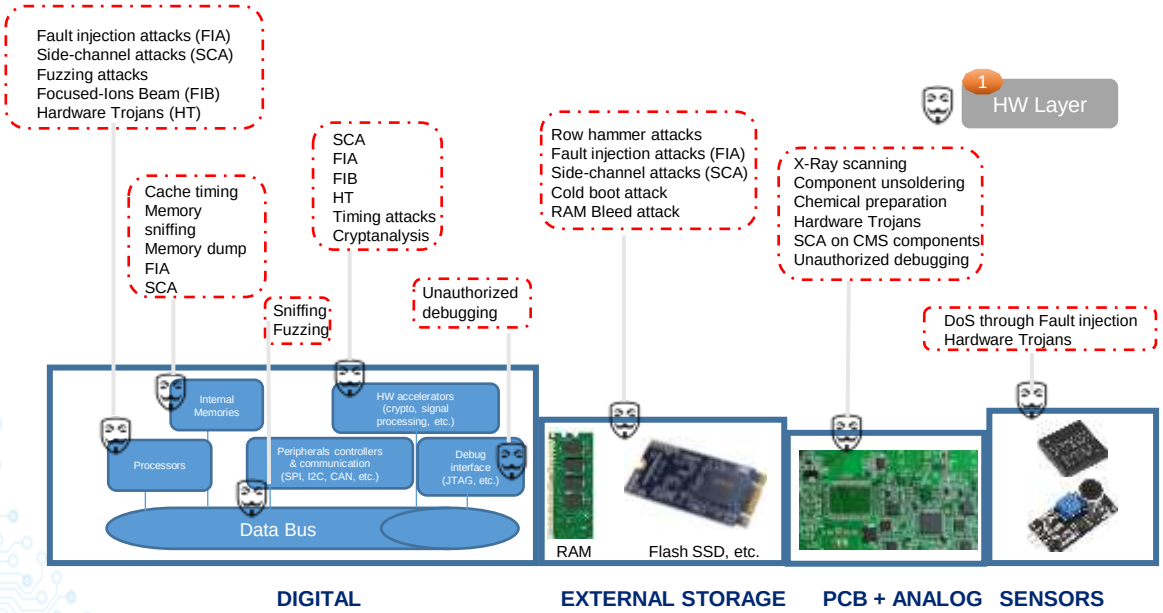
Guide for Conducting Risk Assessments

NIST

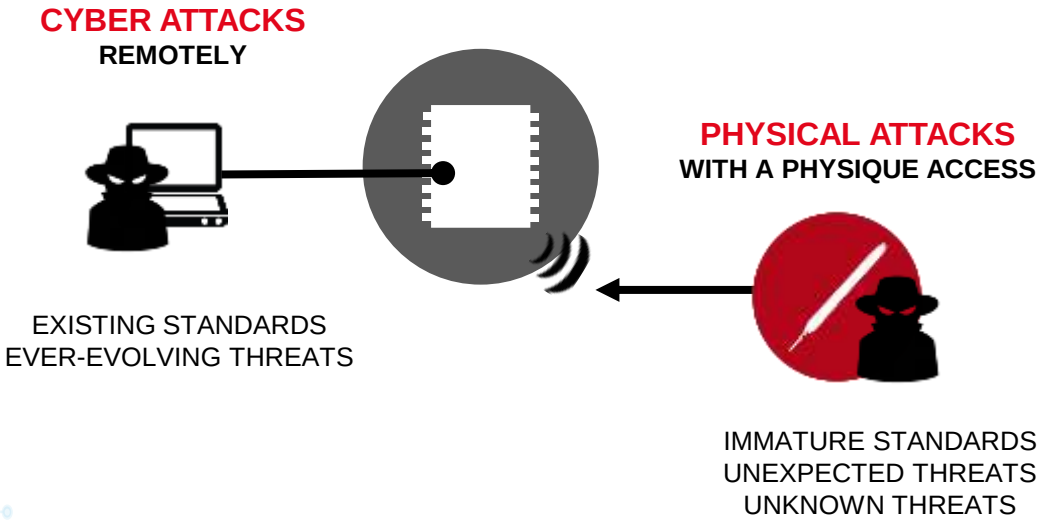
National Institute of Standards and Technology

U.S. Department of Commerce

List of Known Vulnerabilities: HW Layer

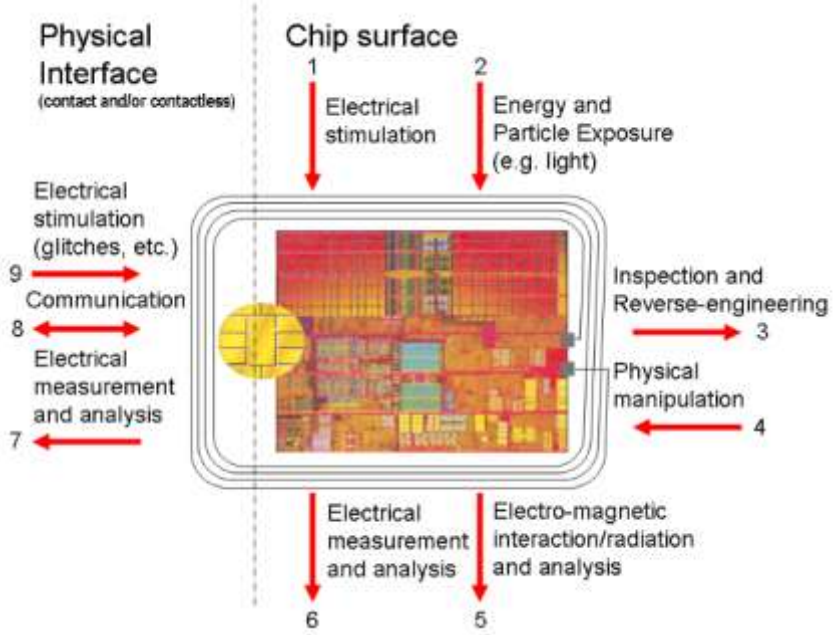


What Kind of Security Are We Talking About?



Example of Smartcard Potential Vulnerabilities

Typical electronic connected device…



Source: PP0084

List of Known Vulnerabilities Per System

Automotive – Smart car example: Multiple layers = multiple risks

- Bus sniffing
- SCA
- FIA
- Fuzzing
- Binary analysis
- Malware injection
- Unauthorized debug

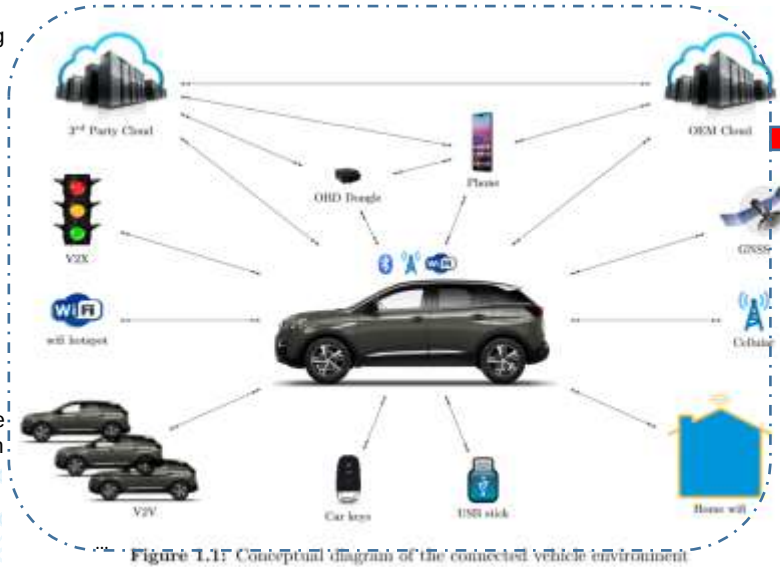
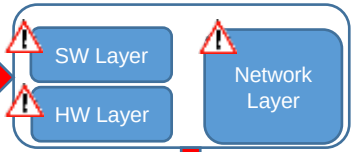


Figure 1.1: Conceptual diagram of the connected vehicle environment

All layers are impacted!



The targeted heart is ECU device

ECU example

First Protection Is Cryptography

- Cryptography is the art of hiding data in the presence of an adversary.
- Cryptography is the study of securing communication.
- **Main Goals:**
  - **Confidentiality:** Sensitive data can be accessed only by users with good keys
  - **Integrity:** Sensitive data can not be altered (modified) by non authorized parties
  - **Authentication:** Confirm that the sensitive data came from the stated sender
  - **Non-repudiation:** Sensitive data sender can not refute the validity of a statement or contract

About Security Threats

Cryptography is robust but Physical Attacks are here …

Passive Analyses

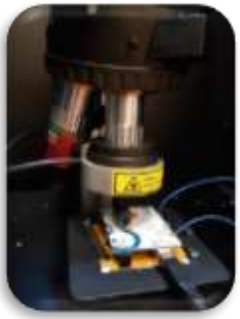
- Do not Interact directly with the target:
  - ➔ Exploit a physical property related to the activity of the sensitive data
- Common analyses: SCA (Side-Channel Analyses)

Active Analyses

- Interact directly with the target:
  - ➔ Access to the target
  - ➔ Perturbate its normal behavior
- Common analyses: FIA (Fault Injection Analyses) / Active Probing (FIB)

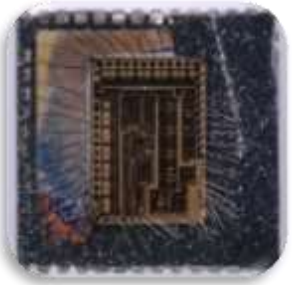
Versatile Analysis/Attack Methods

voltage glitch



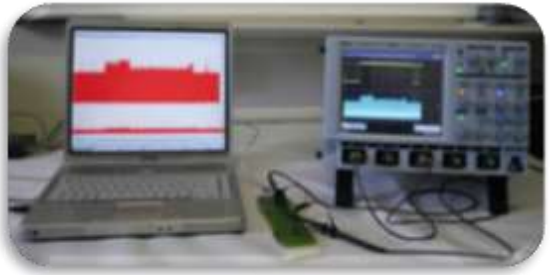
laser

photonic emission analysis



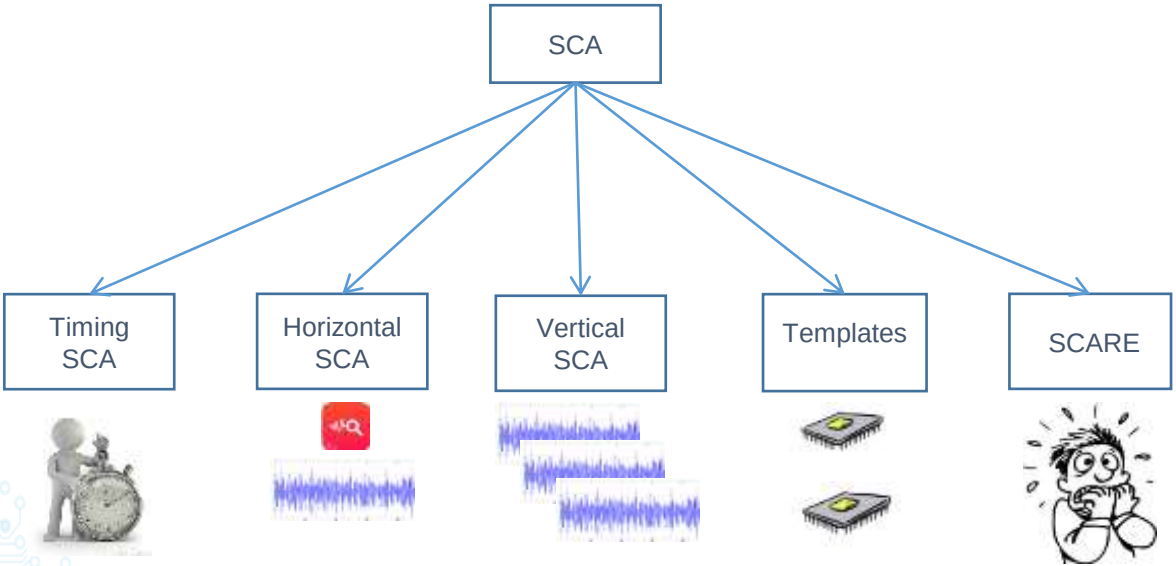
decap

electromagnetic pulse injection



power analysis

SCA Classes


SCA
Timing SCA
Horizontal SCA
Vertical SCA
Templates
SCARE

Fault Injection Attacks Principle

- For a unique goal: provoke a fault

2+2=4

- And find a secret information as a key, a signature …
- Or bypass a sensitive operation as pin code

2+2=3

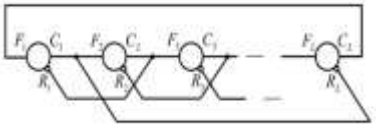
TRNG (True Random Number Generator)

TRNG Application

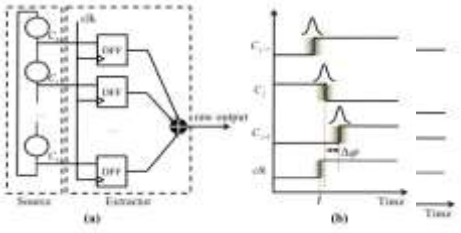
- Authentication
- AES/SM4 IV(Initialization Vector)
- AES/SM4 Masking
- RSA/ECC Key Generation
- RSA Random Modulus/Exponent
- ECC Random Scalar/Projective coordinate

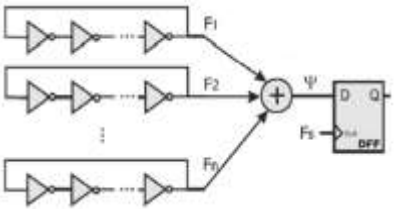
TRNG Standard

- BSI AIS21/31
- NIST SP800/90B
- GM/T0062-2018
- GM/T0078-2020

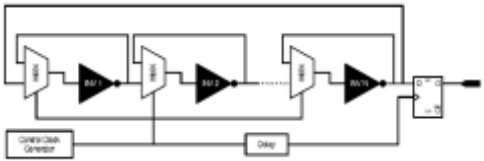


Self-Timed Ring TRNG





XOR Ring TRNG

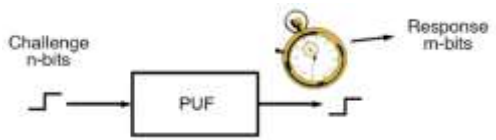


MUX Ring TRNG

PUF (Physically Unclonable Function)

PUF Criteria

- Robustness(Reliability)
- Randomness(Unpredictability)
- Uniqueness(Individuality)

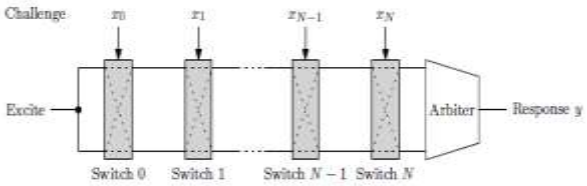


PUF Type

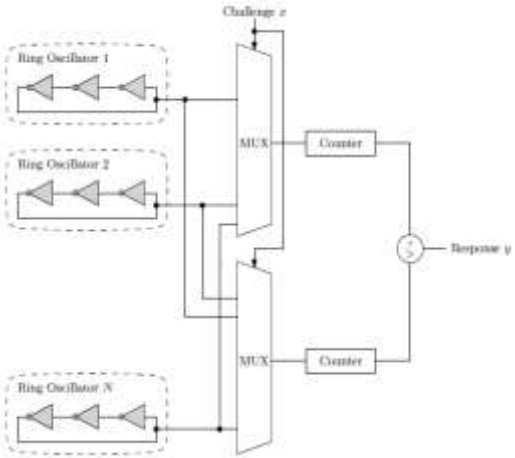
- SRAM PUF
- OTP PUF
- Latch PUF
- Delay PUF

etc.

PUF vs NVM ID



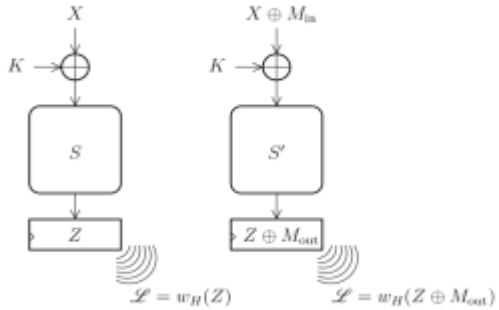
Arbiter PUF



Ring Oscillator PUF

SCA Countermeasures – AES/SM4

- **Embedded hardware countermeasures based on Masking**
- **Implemented at front-end phase**



Side-channel leakage L in a block cipher, unprotected (left), and masked (right)

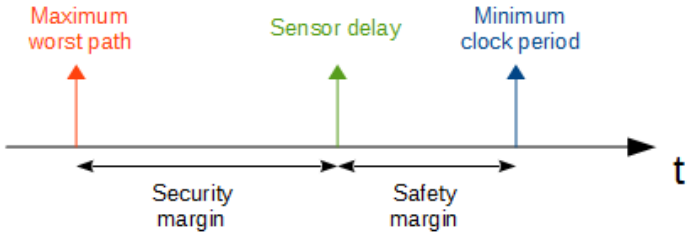
Where :

- X is the plaintext
- K is the Key
- Z is the cipher text
- M is the mask
- wH the hamming weight.

Fia Countermeasures – Digital Sensor

- **Detects abnormal environmental change that might have an effect on the circuit's normal operation**

- **One principle:**
  - An artificial path is added in the circuit. It is designed to be critical, and becomes an active probe, that runs at the same velocity than the rest of the circuit



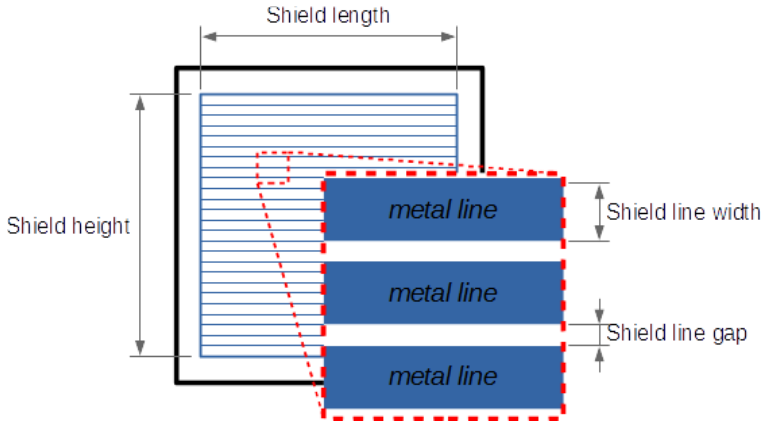
- **Implemented during the back-end phase**

Tampering Attack Principle

- **Tampering attack**
  - Wire micro-probing to read or force an equipotential
  - Wire cutting (e.g., non-redundant alarms, entropy source disconnection from a true random number generator)
  - Wire re-routing
  - Feature removal
  - Burnt fuses opening
  - Functional modification of the crypto to make it weak (see "bug attack", for instance)
  - Altering of the ROM boot code

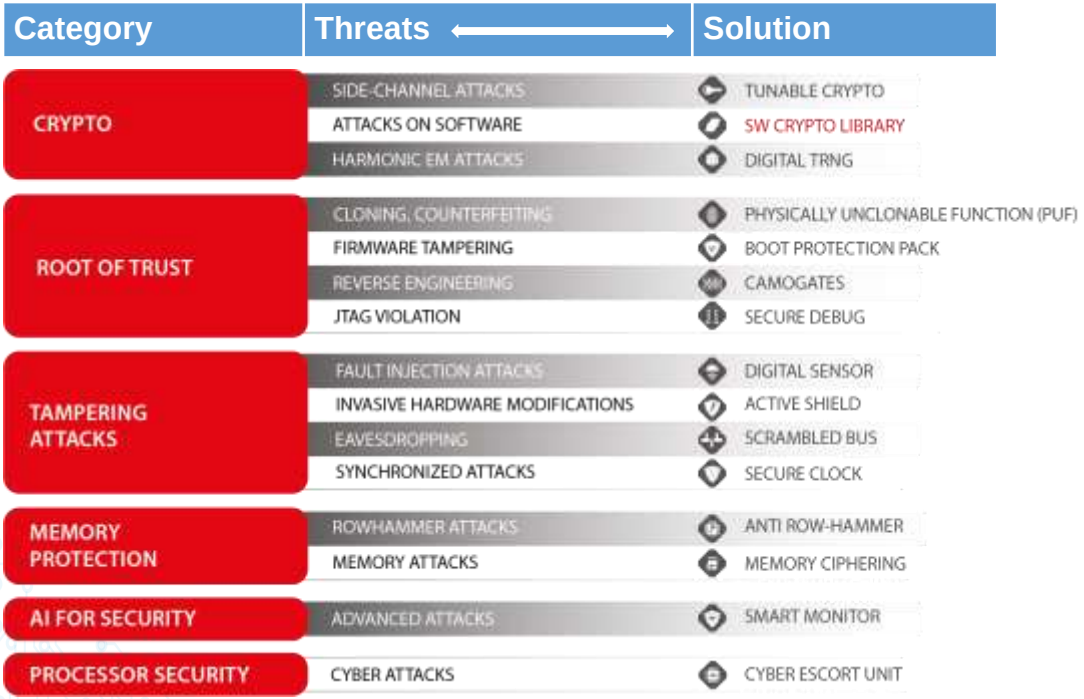
Tampering Attack Countermeasures – Active Shield

- Place a mesh over the sensitive portions of the circuit
- Active monitoring the mesh's integrity using random cryptographically-generated patterns to detect integrity violations



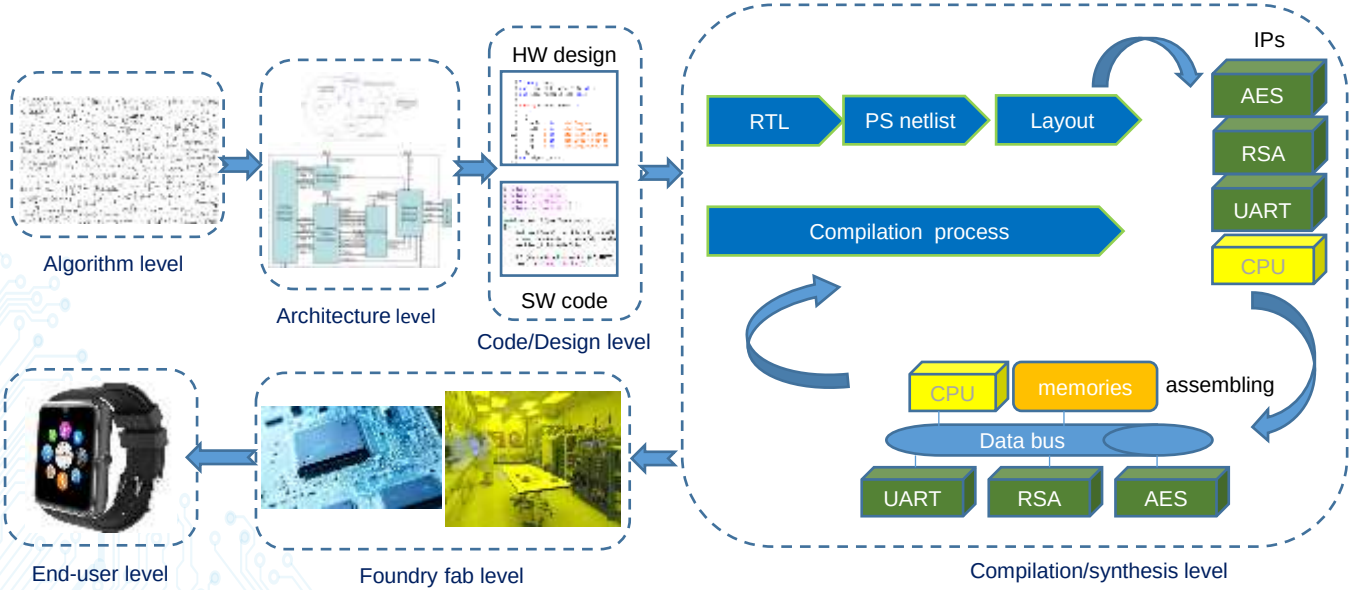
- Implemented during the back-end phase

Map Each Threat To Its Solution

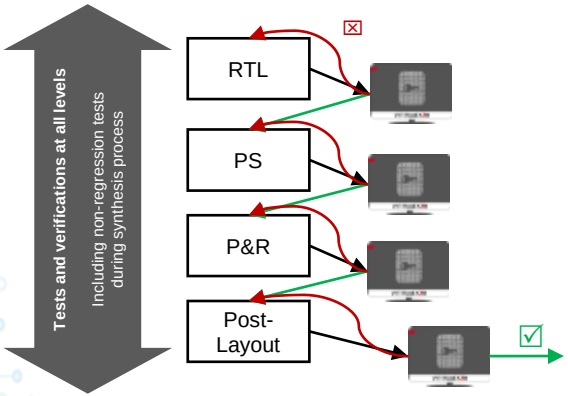


- **SECURITY TESTING IN THE LIFE-CYCLE**

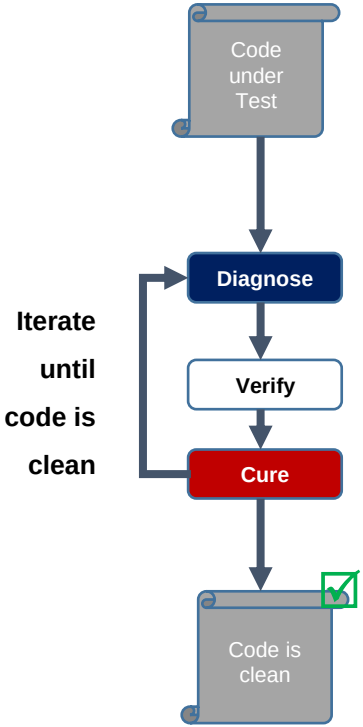
✓ Embedded cyber system life Cycle and Levels



Verify Your Design All Along The Development



For hardware…



For hardware and software…

Acknowledge

THANK YOU !

A World-Leading ASIC Design Solution Provider

Email: sales@britesemi.com
Tel.: +86 21 5037 6566