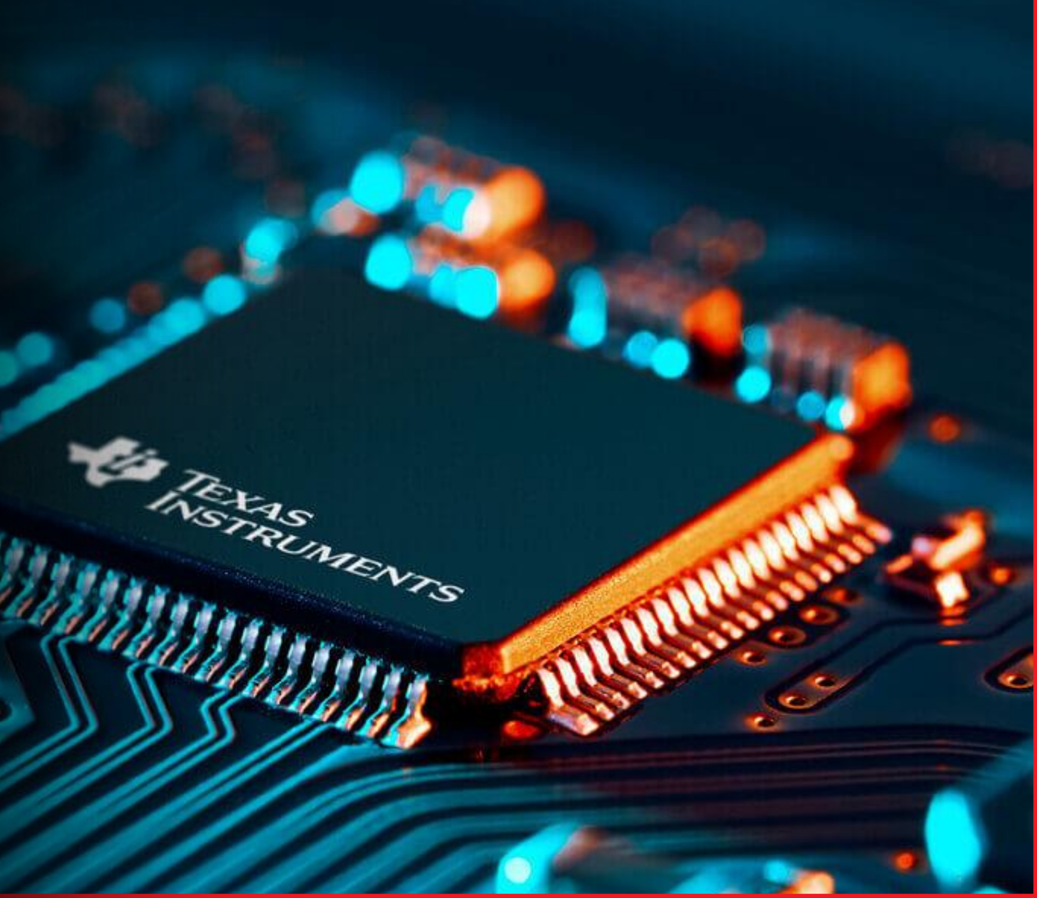
Texas Instruments

2024 Embedded Seminar

Prepare for security regulations: 3 steps to take now



Ron Birkett

Processor Software Product Manager

Security basics and enablers

THREATS

THEFT

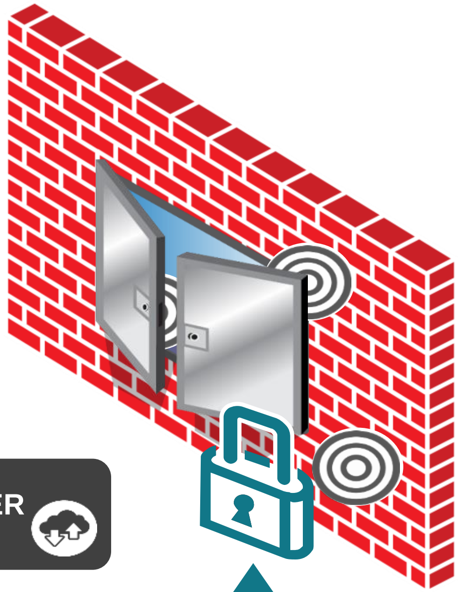
CONTROL

EXPOSURE POINTS

STORAGE

RUN-TIME

TRANSFER



ASSETS

IDENTITY & KEYS

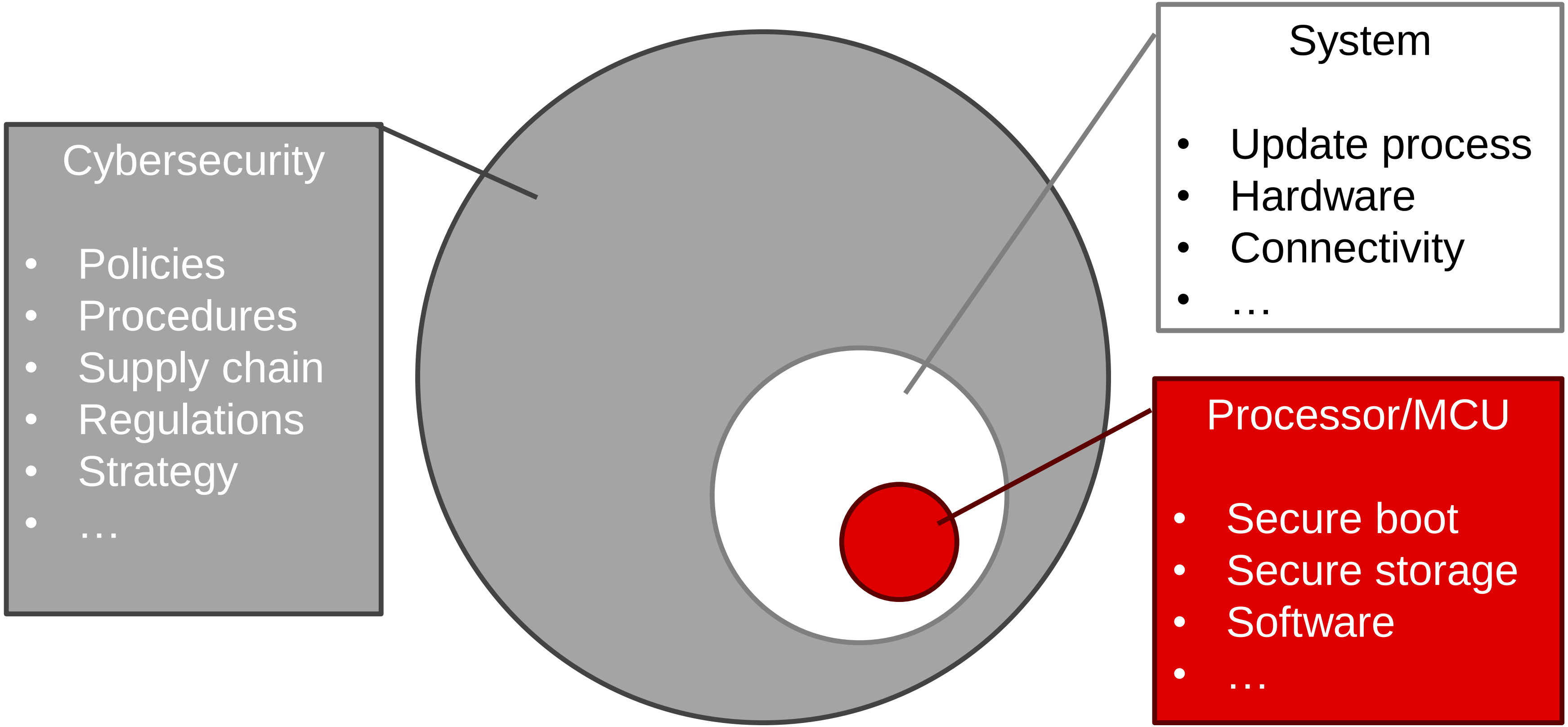
DATA

CODE & IP

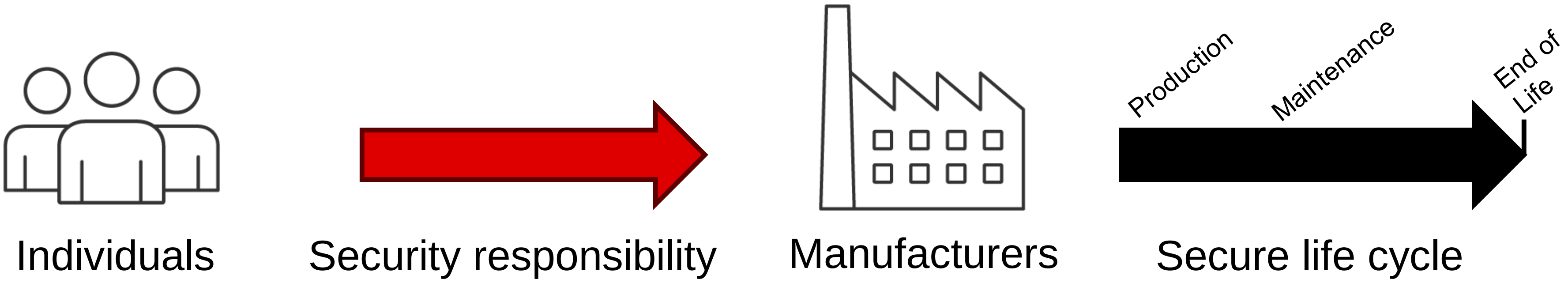
TI SECURITY ENABLERS

"TI's security toolbox of **security enablers** helps address the emerging threats of an increasingly connected and complex world"

Cybersecurity is a large space



Security regulations

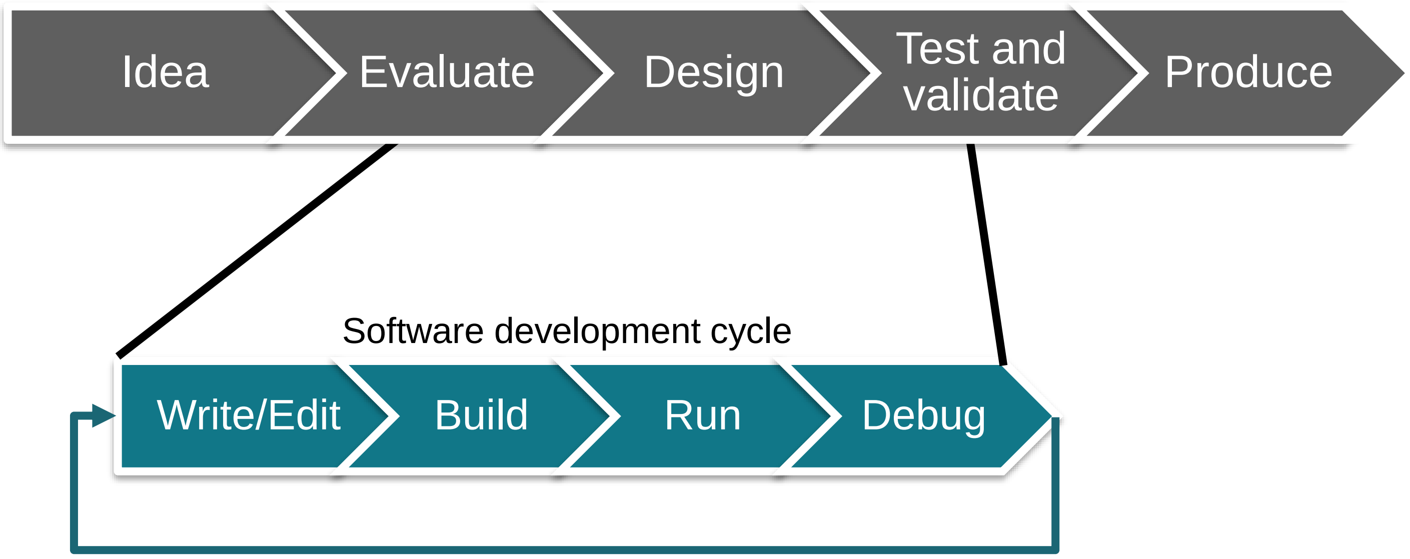


- The **connected** nature of modern devices is driving a need for **better security**
- Nation states are concerned that threats could have a **large impact**
- Individuals are not equipped/educated to secure devices themselves
- Latest **regional regulations** (i.e. EU Cyber Resilience Act) shift responsibility to **manufacturers** with possible **fines** and/or **other actions**
- Responsibility includes **maintaining security** for a defined, published timeline
- Requirements are broad from **design practices** to **disclosing vulnerabilities**

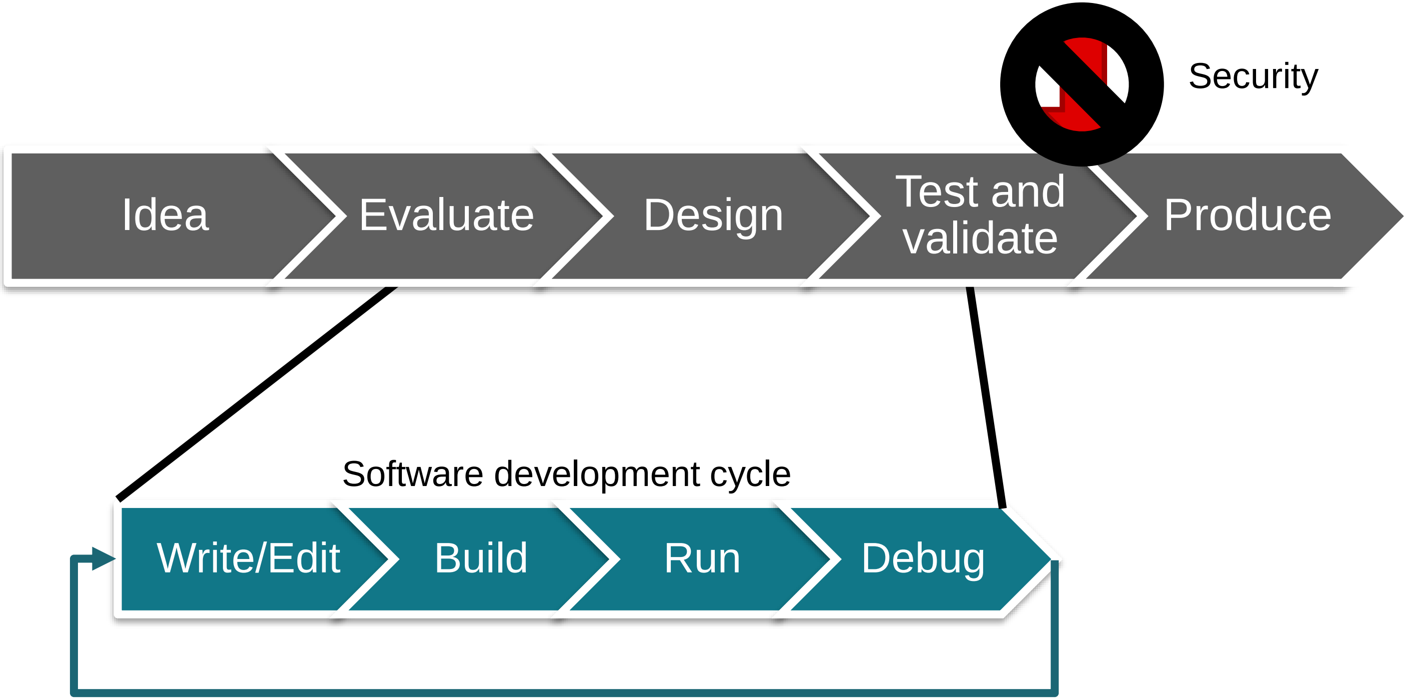
Three things to consider now

1 Secure by design

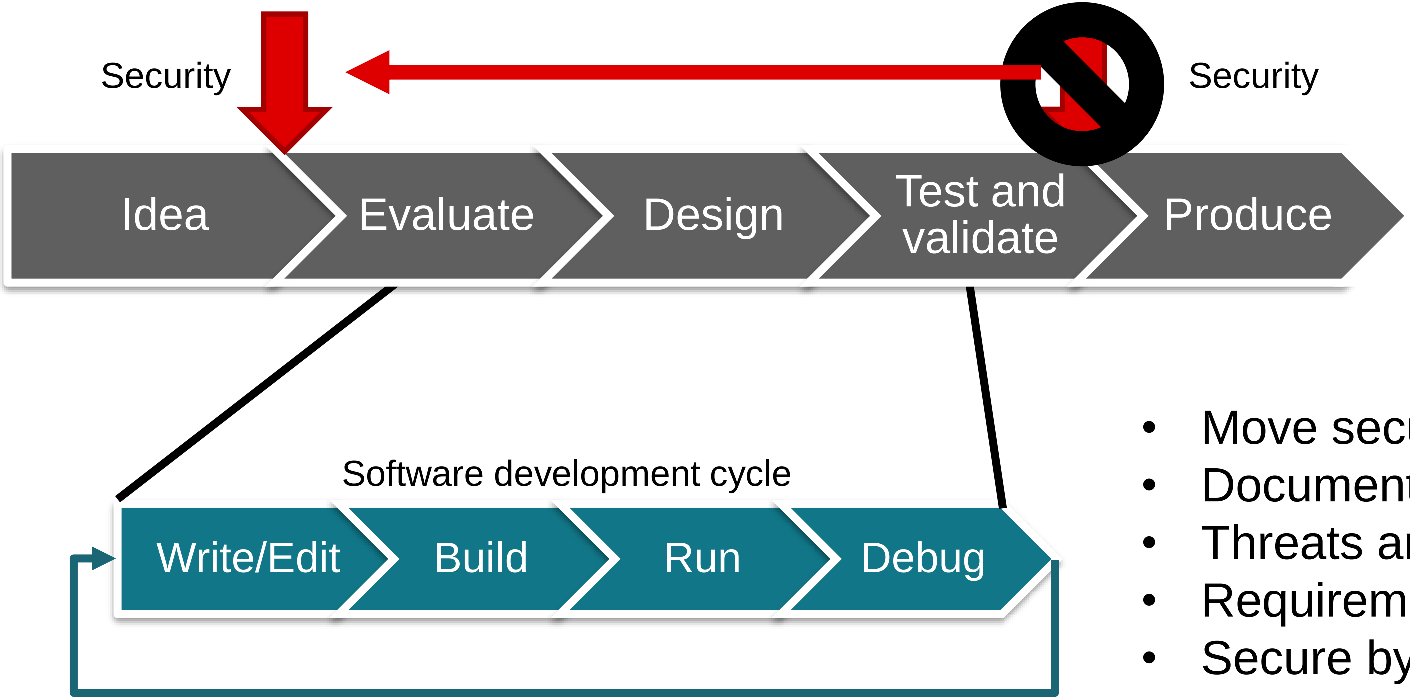
A typical development flow



Security is not a bolt-on!

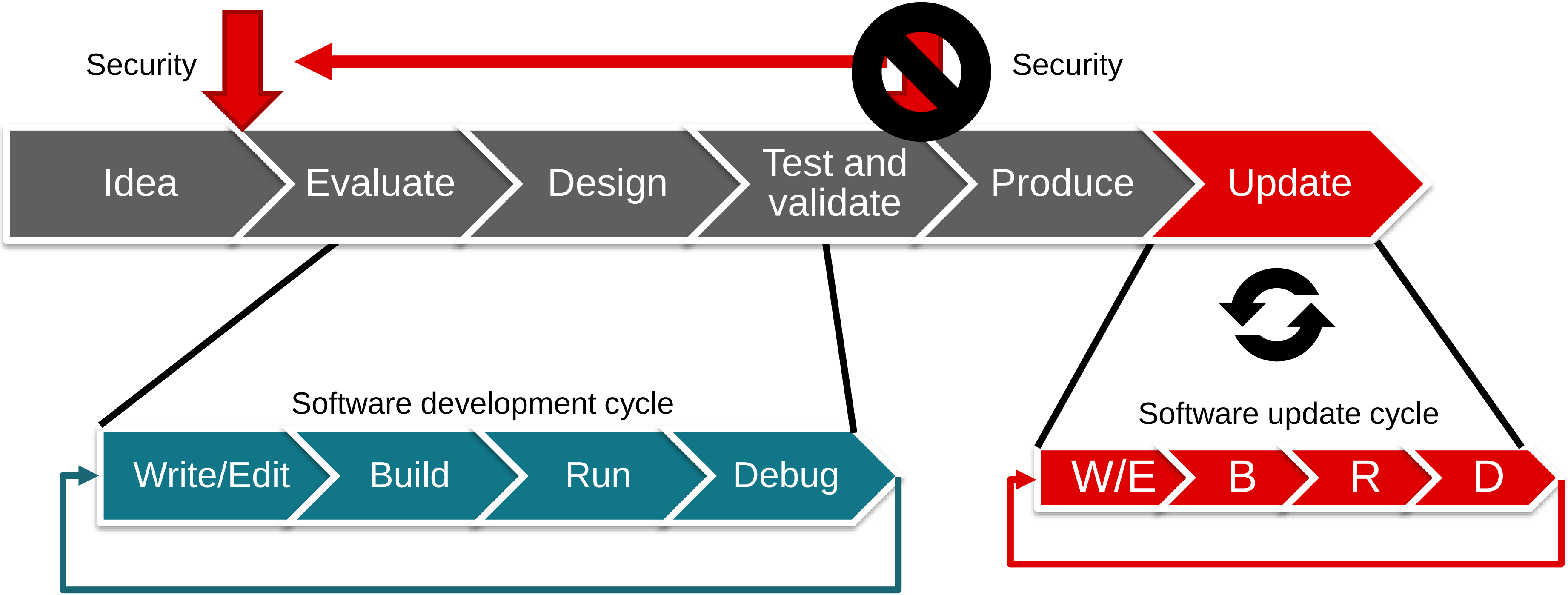


Security impact on development flow

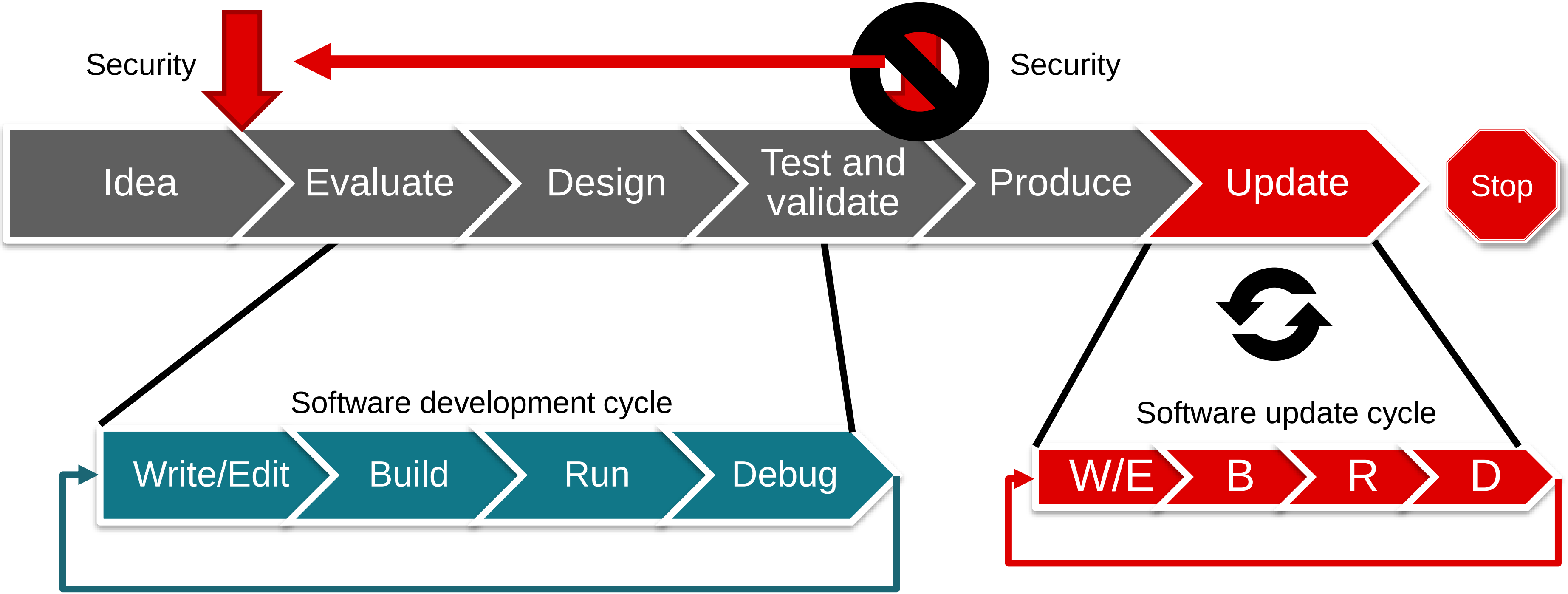


- Move security to beginning
- Documentation
- Threats and risks
- Requirements
- Secure by design

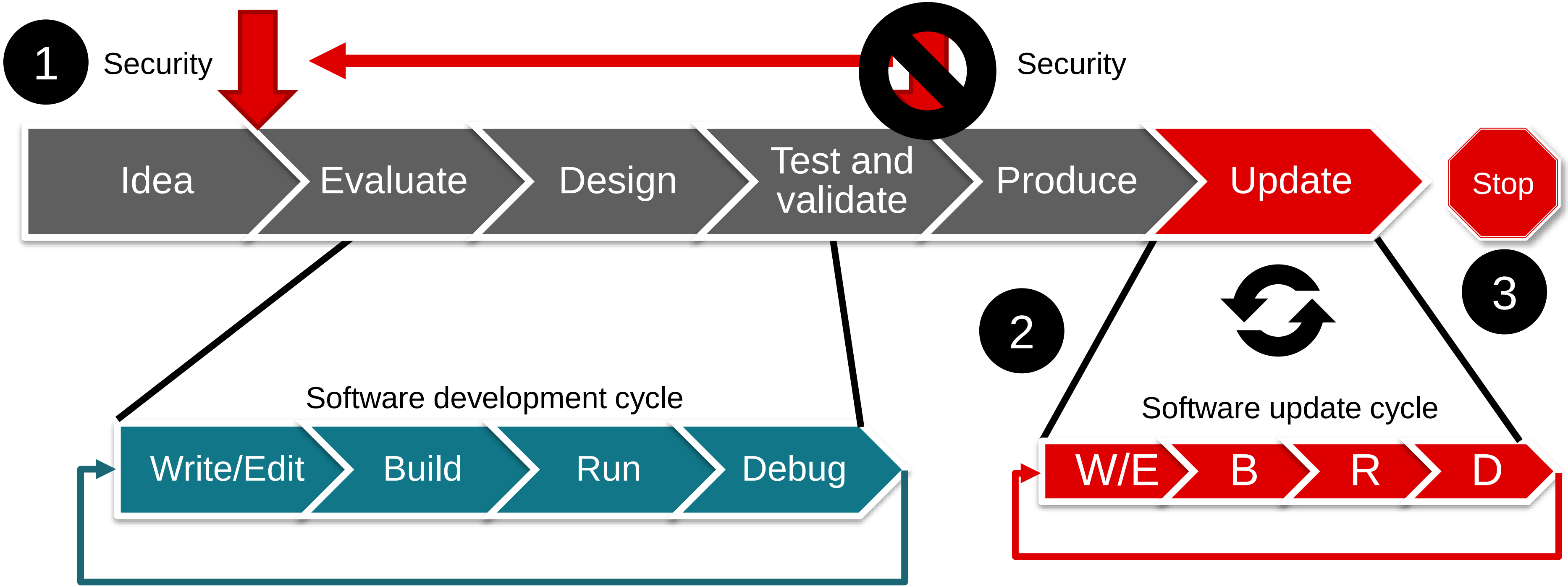
Adding updates



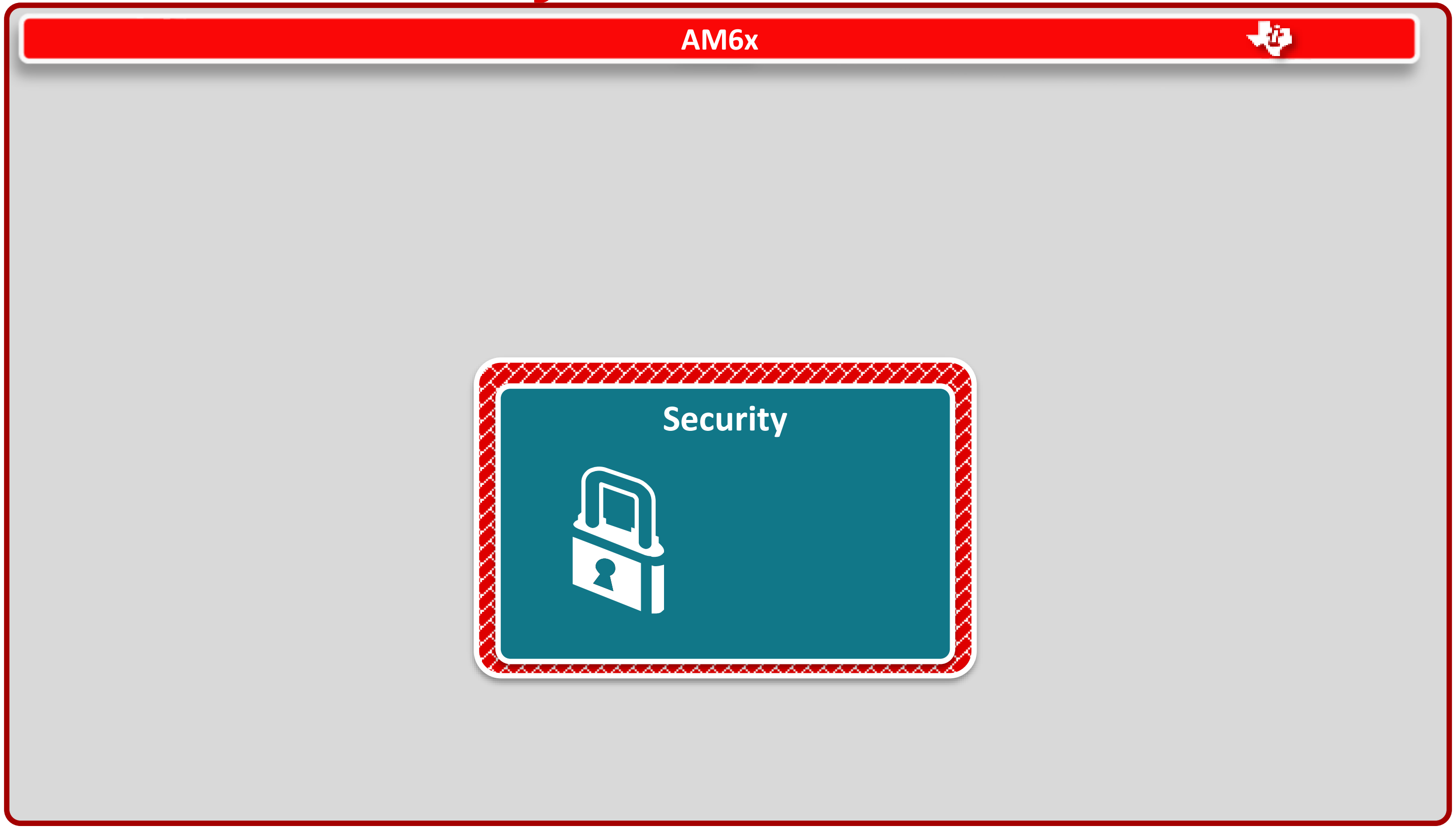
Defining life cycle



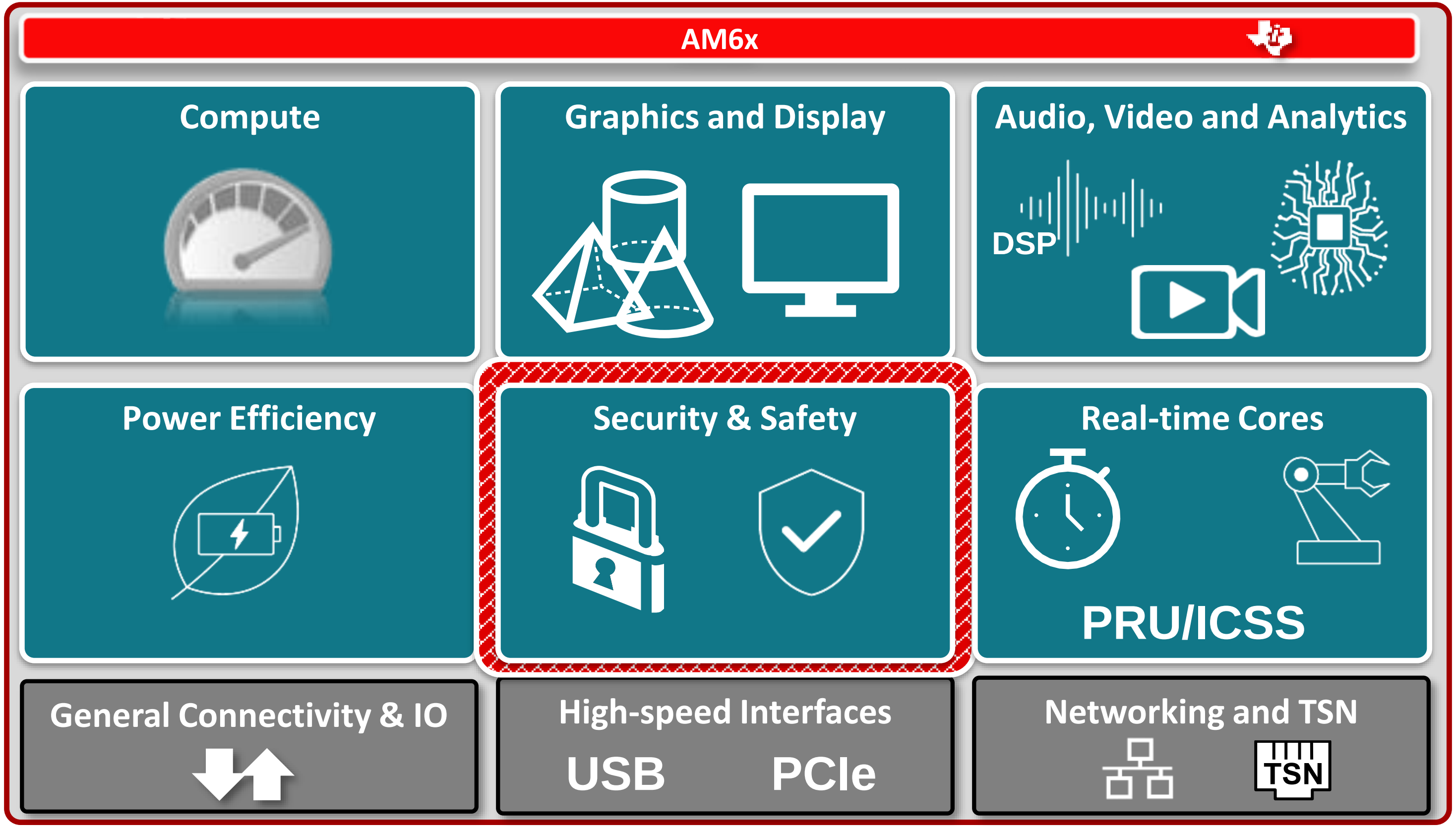
Security impact on development flow



TI processor security



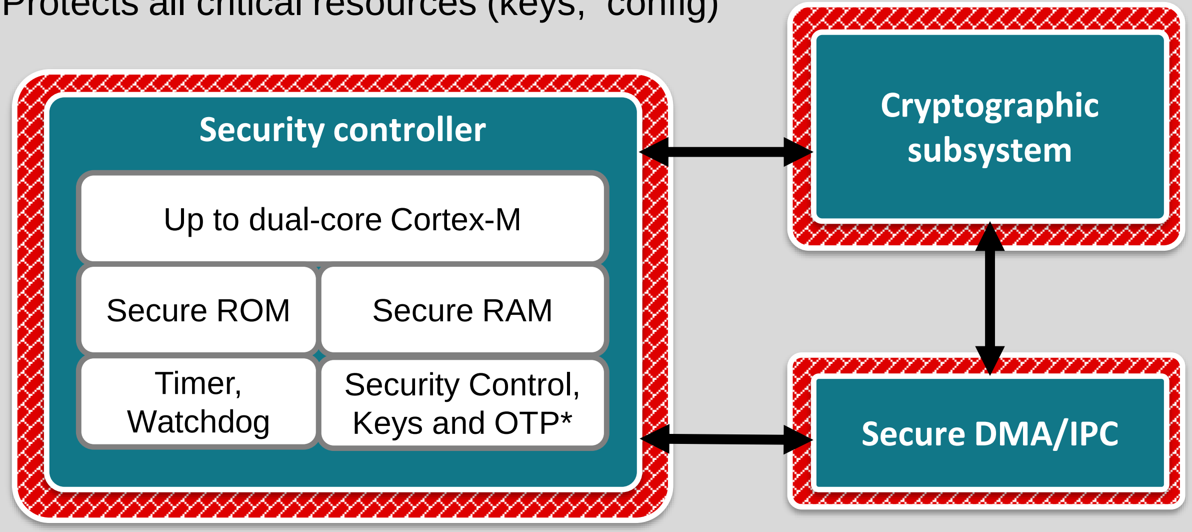
TI Processor Cortex®-A based architecture



TI Processor security architecture

AM6x

- Central control for security (secure boot, debug, etc.)
- Isolated from the rest of the system by firewalls
- Protects all critical resources (keys, config)



* OTP = One-Time Programmable Memory

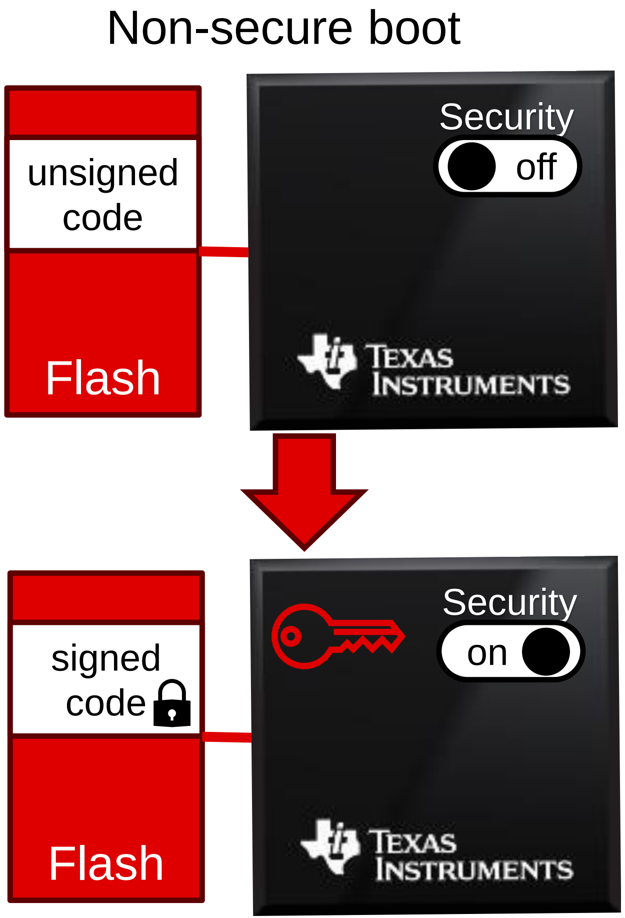
Three things to consider now

1. Secure by design
2. Secure boot

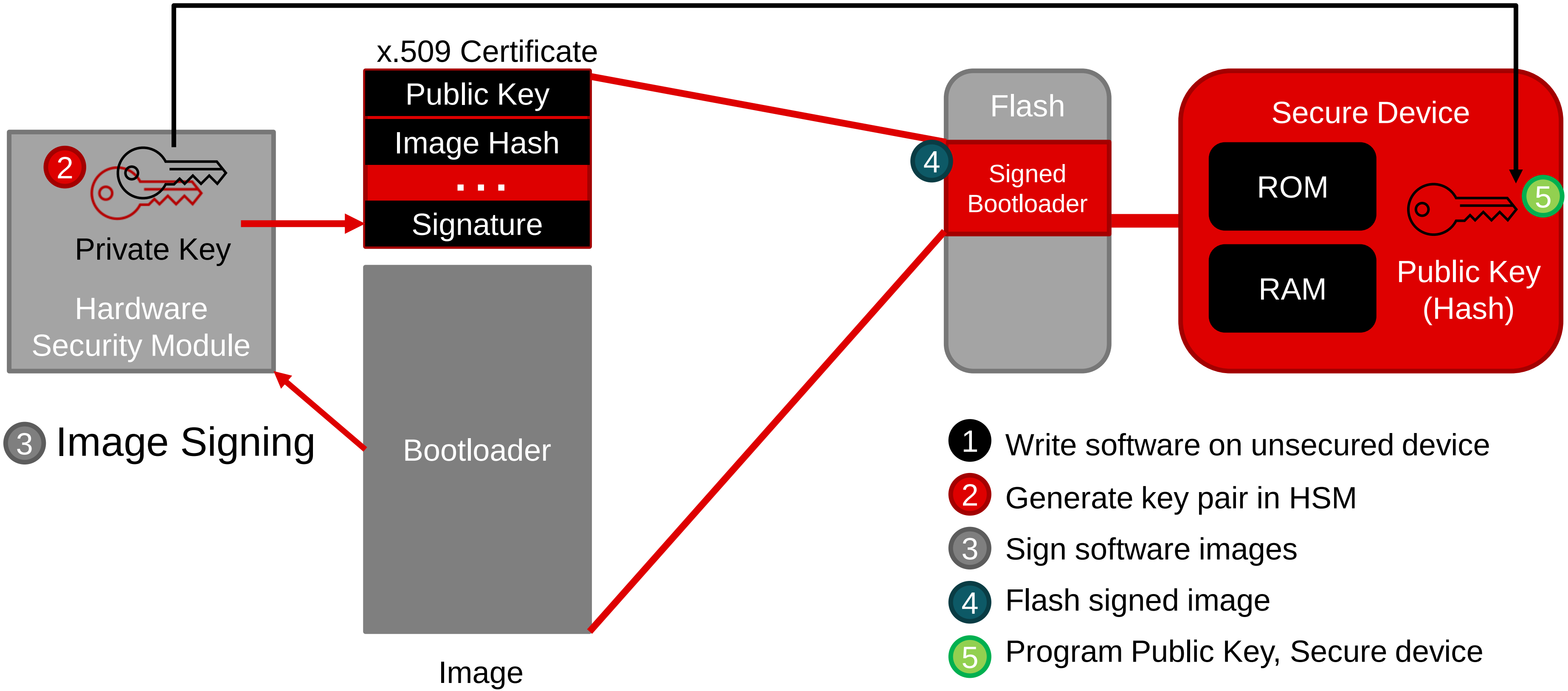
Secure boot

Secure boot is a **hardware based "Root of Trust"** to authenticate and protect boot code and data. Customers program their own keys using software/tools supplied by TI.

- When security is enabled, the device will only boot code specifically prepared for the device using asymmetric encryption and hashing
- Takeover protection
  - My device only runs **my software** (authenticity and integrity)
  - Non-volatile one-time-programmable memory within device is configured so device will only boot **"trusted" software**. Ensure external flash content is not modified.
  - Overwriting flash or changing the boot source to load new code that is not signed will result in a **boot failure**
- **Chain of Trust** can be extended to following boot stages (i.e. OS or Application Image)



Steps required for secure boot

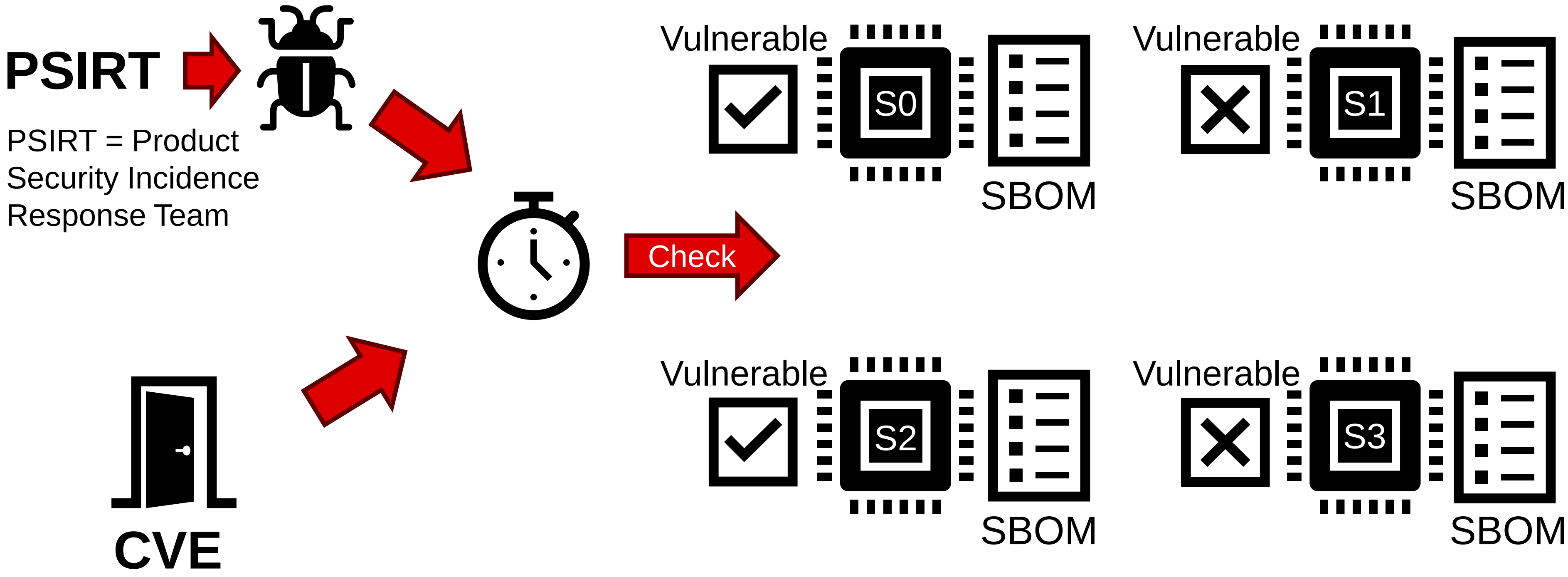


1. Write software on unsecured device
2. Generate key pair in HSM
3. Sign software images
4. Flash signed image
5. Program Public Key, Secure device

Three things to consider now

1. Secure by design
2. Secure boot
3. SBOMs

Vulnerabilities and exploits

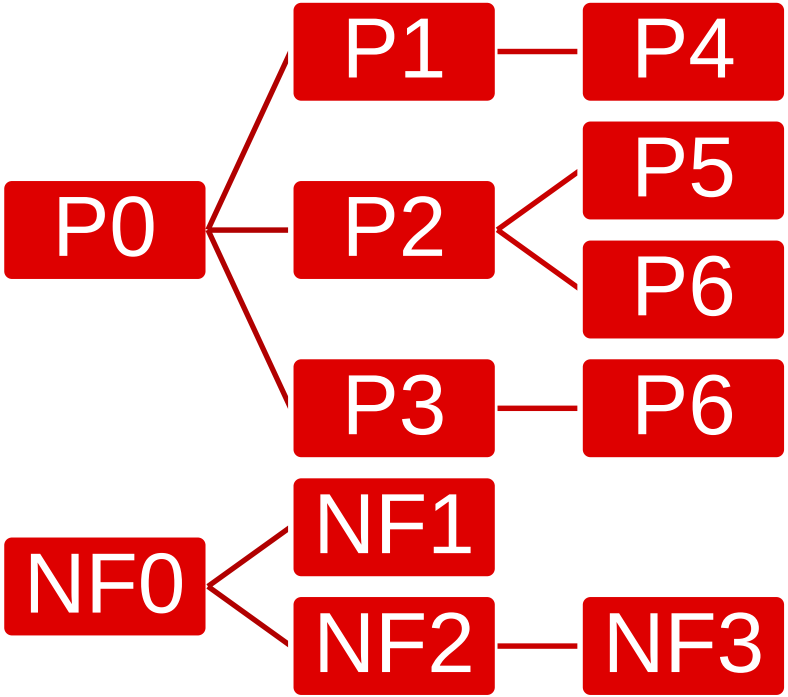


CVE = Common Vulnerabilities and Exposure

SBOM = Software Bill of Materials

Transparency in the software supply Chain

SBOM



- List of packages and dependencies
- Versions & patches
- How to organize (device, build, etc.)
- Different formats (ex. SPDX)
- Can be generated by build system
- Binary scanners as well

Centralized DB by device ***quickly*** reveals vulnerable systems and enables automation…

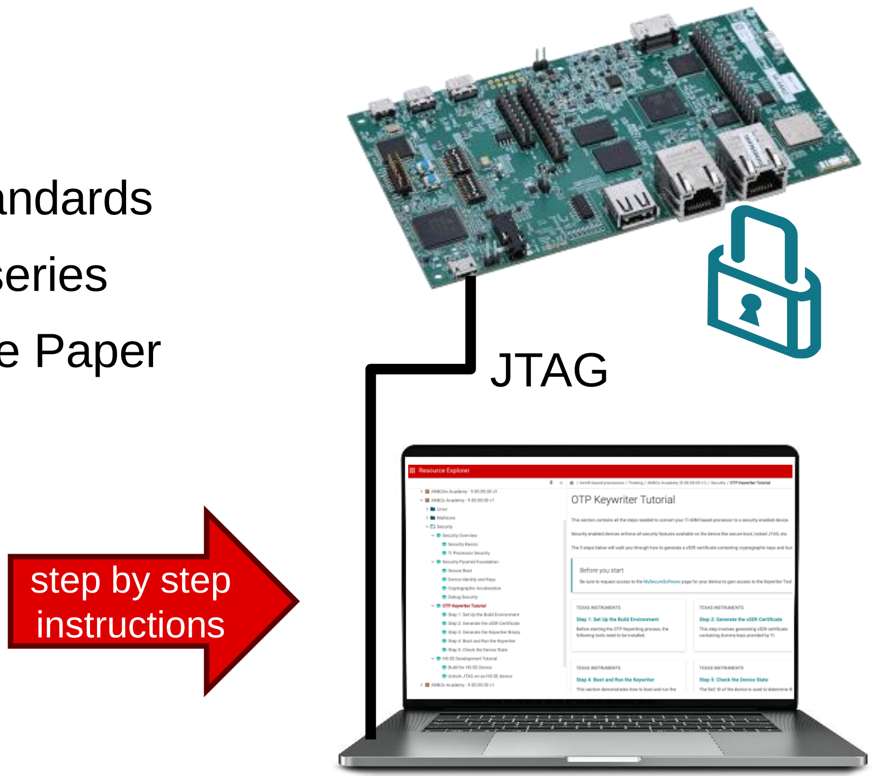
Three things to consider now

1. Secure by design
2. Secure boot
3. SBOMs

Going further…

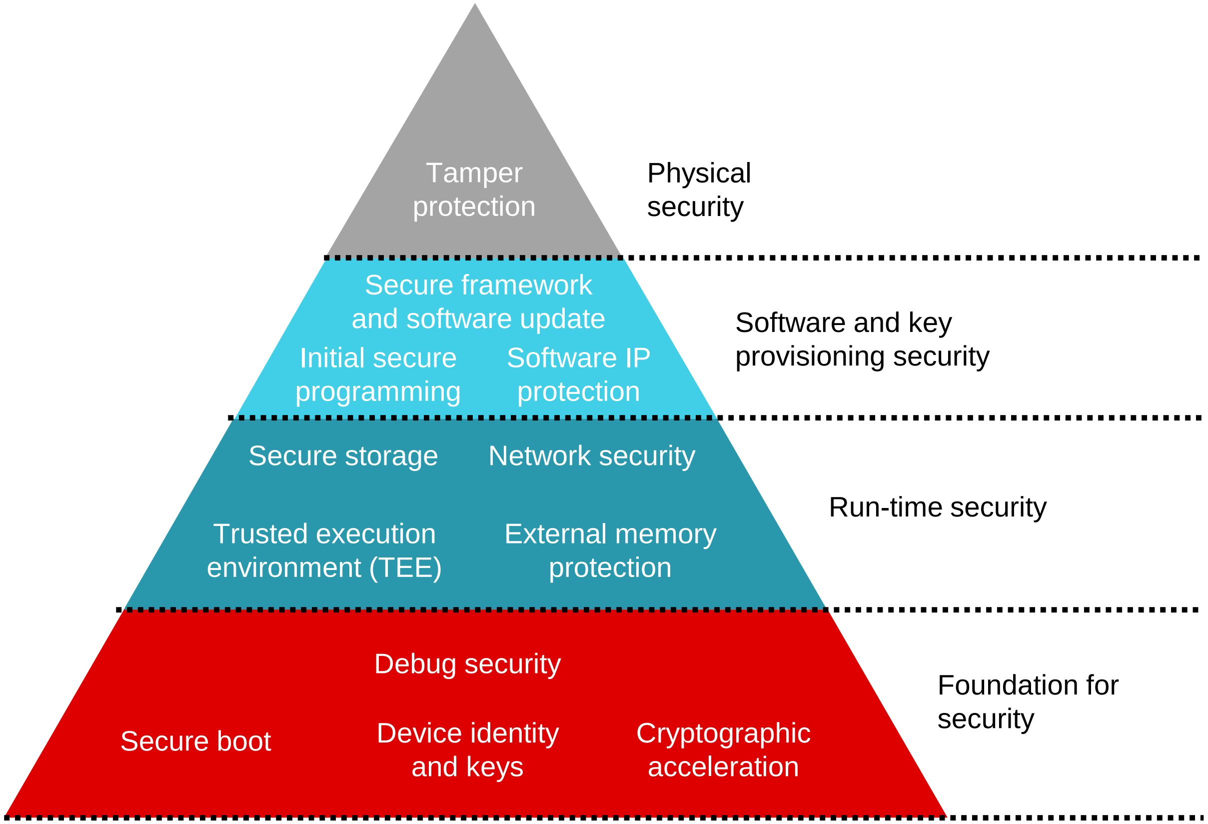
- Standards themselves
- A great comparison of CRA to existing standards
- TI Foundational Security Enablers video series
- TI Securing ARM Based Processors White Paper
- TI Security Academies

Device	Academy
AM62x	Link
AM62Ax	Link
AM64x	Link
AM67x	Link



Thank You!

Security enablers in embedded systems



Device Types – simplified development flow

General purpose (GP)

- Device not used for secure operation
- No security switch, security features disabled and cannot be enabled
- JTAG enabled (unlocked)
- Crypto cores enabled

GP device cannot be changed to HS

High security (HS)

HS - FS

- Field securable (FS)
- Development and testing
- No secure boot
- JTAG closed only for security controller
- Security largely disabled

non-reversible
OTP writing

HS - SE

- Security enforced (SE)
- Production
- Enforce secure boot
- JTAG closed completely
- All available security features active

HS-FS device type is shipped from TI for HS and typically included on EVMs

Processor security feature highlights

- **Security controller**
  - Up to Dual-core security coprocessor for centralized security control
  - Reduces attack surface for critical assets (e.g. Keys)
  - Dedicated, Crypto channel, DMA and IPC for HSM
- **Field securable (HS-FS) device type**
  - Device behaves as non-secure device until the keys are programmed
  - Helps customers test their hardware prior to productization with secure keys
- **Secure boot**
  - Customer can program hardware (efuse) keys themselves
  - Supports encrypted and authenticated boot
  - **Uses industry standard x509-based booting certificates**
- **Dual root key support**
  - Support for two sets of hardware (efuse) root keys
  - Enables customers to switch to a new root key in the field
- **Enhanced firewall architecture**
  - Dynamic access control to all SoC resources (memories, peripherals, cores, etc.)
  - Provides the ability to promote or demote access to resources
- **Smart cryptographic subsystem**
  - Chinese Crypto support
  - ECDSA and DRBG standards hardware support, in addition to AES, 3DES, SHA1/2, MD5
  - Ability to proxy security master (e.g. SMS) to promote or demote incoming data streams
  - Improved performance with ability to push data streams to secure world with minimal context switching
- **Enhanced debug control**
  - Security aware debugging (e.g. ability to lock secure world while debugging public world)
  - SMS controlled challenge-response protocol for opening debug

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265