FTF 2016
TECHNOLOGY FORUM

SECURITY VS FUNCTIONAL SAFETY

FTF-AUT-N1814

RICHARD SOJA
SYSTEMS ENGINEER, AUTO MCUs AND PROCESSORS
FTF-AUT-N1814
MAY 18, 2016

PUBLIC USE

AGENDA

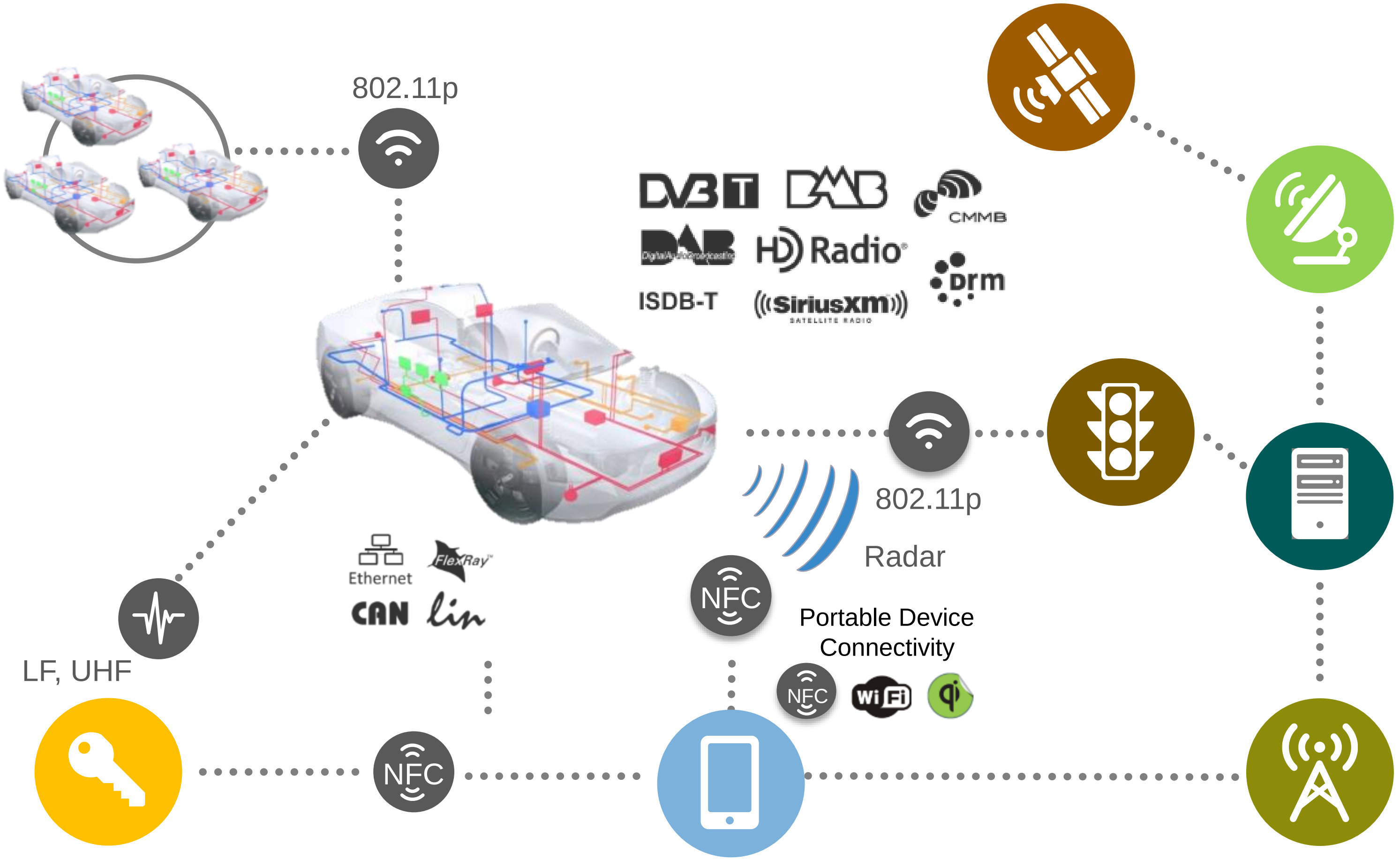
- Motivation for Safety and Security
  - Attacking the Connected Car
- Safety & Security Definition
- Complementary or Contradictory?
- Hardware Fault Examples & Solutions
- Safety & Security Processes
- NXP History in Security & Safety
- NXP Automotive Product Offerings

The Connected Car

A Cloud-connected Computer Network on Wheels

- A networked computer
  - up to 100 ECUs per car
  - and many sensors
  - inter-connected by wires
  - more and more software

- Increasingly connected to its environment
  - to vehicles & infrastructure
  - to user devices
  - to cloud services



…is an Attractive Target for Hackers!

Easy Access

- Fully Connected Car
- External & internal interfaces
- Wired & wireless interfaces

Prevent Unauthorized Access

High Vulnerability

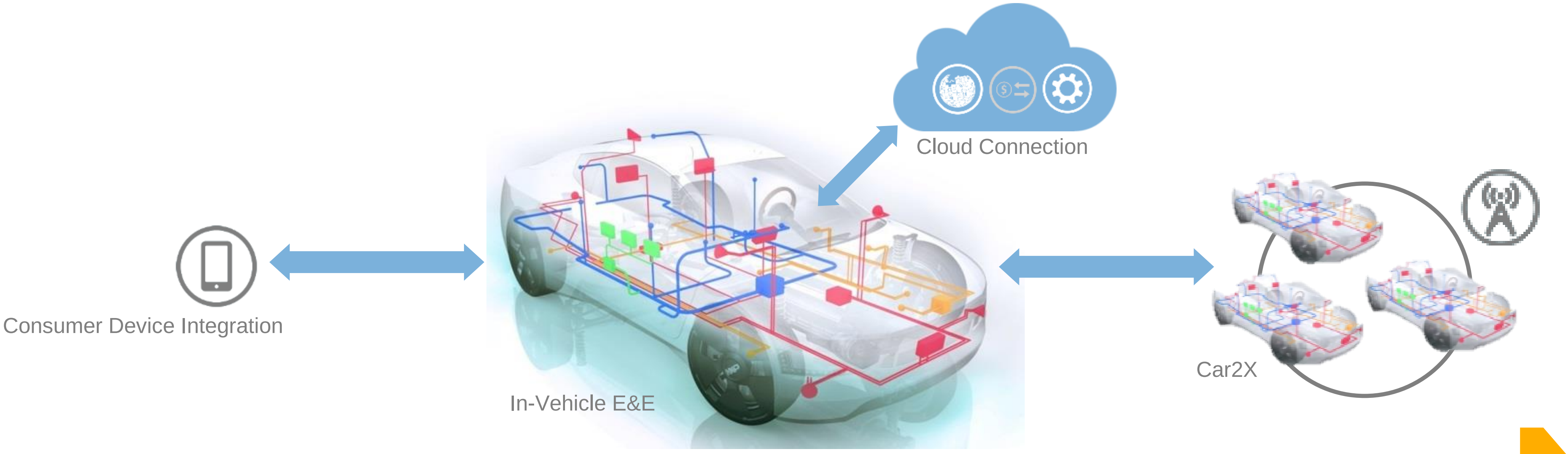
- Increasing number of nodes
- More advanced features
- X-by-Wire

Increase Safety

Valuable Data

- Collection of data/info
- Storage of data
- Diagnostic functions

Protect Privacy



Cloud Connection

Consumer Device Integration

In-Vehicle E&E

Car2X

What is Safety and Security?

- Safety is a state of being
  - Safety is subject to the forces of nature, and is impacted by natural events
  - While unpredictable in time, the causes and effects of the events are well understood and quantifiable
- Security is a means to achieve that state - services and functions
  - Security is subject to the forces of good and evil, and is impacted by human actions
  - These actions are somewhat predictable, and usually much more targeted than natural events
- Some languages may not differentiate between the words “Safety” and Security”
  - e.g. German “Sicherheit”, Spanish “seguridad”
  - This might make it difficult to explain the differences in the context of vehicle systems

Mitigating Security and Safety Violations

- Analysis of all components in the system, plus rigorous adherence to well defined development processes can protect against and mitigate the effects of safety and security violations
- One can put up barriers to counter safety and security attacks, but if they fail, mitigation of the consequences of the attacks must come in to action.
- Trade-offs are made between the cost of these countermeasures, and in the case of security, the cost of the attack and the benefit to the attacker

Safety

- Safety is associated with the avoidance of physical harm (to human beings)
- Safety measures in vehicles include:
  - ABS braking, Seat belts, Collision avoidance, Non-flammable construction, Reinforced body panels, etc.
- For vehicle electronics, “safety” means that no harm will result in the event of an electronic malfunction.
- Safety analysis must be done to determine the cause and effect of electronic malfunction.
  - Many malfunctions will have no effect on the safety of the vehicle.
    - Do not try to over-engineer a solution that has no real value.

Security

- In the context of vehicle control systems, security is associated with controlling access to the vehicle and protecting confidential material
  - Confidential material could be stored in the cloud as well as in the vehicle
- Unauthorized access to the vehicle could result in
  - Physical theft of the entire vehicle or its sub-components
  - Undesired behavior of the vehicle through unauthorized installation of malware

Safe and Secure?

- A person locked in a lion’s cage with the lion may be very secure, but completely unsafe.
  - The security and safety goals are in conflict, due to lack of use case understanding!
- Applying this to vehicle electronics systems, ensuring messages are authenticated does not guarantee safety of the system if there is no underlying fault detection and containment for the safety critical control systems

Secure and Safe?

- A locked treasure chest, teetering on the side of a cliff, may be only temporarily secure, because it is in an unsafe state.
  - The security of the system may be compromised due to lack of safety measures!
- Applying this to vehicle electronics systems, if the security system has no underlying physical fault detection and containment, it may be compromised by that fault.

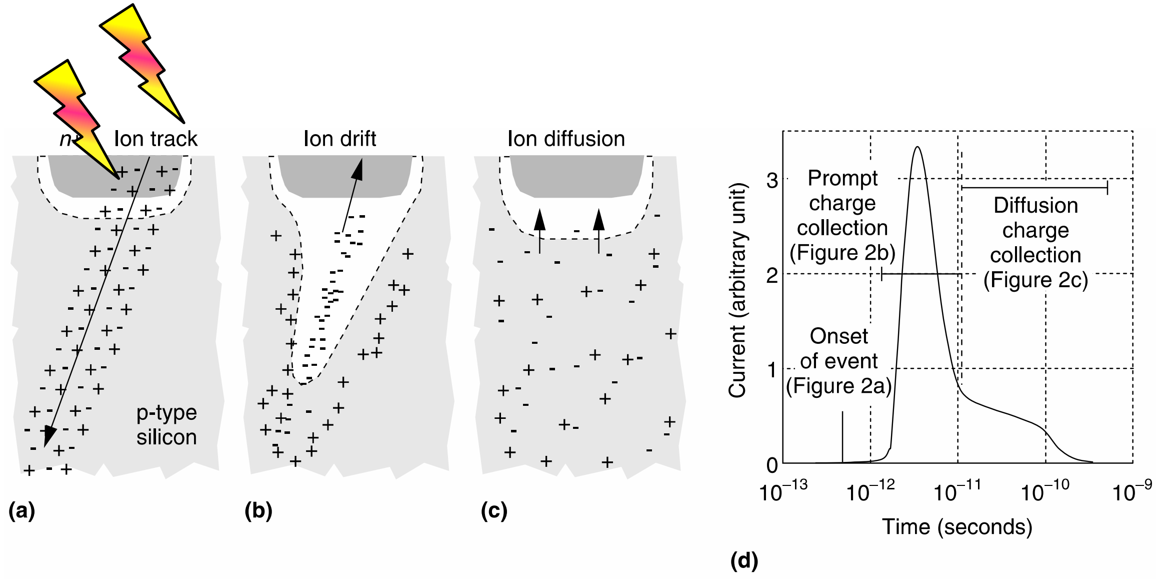
Complementary or Contradictory?

- Contradictory?
  - Safety needs access to vehicle electronics resources to validate correct operation
  - Security needs to restrict access to vehicle electronics to protect confidential material
- Complementary
  - Safety development processes (e.g. ISO 26262) can be added to normal V shaped development lifecycle model.
  - Security can follow a similar methodology
  - Events that cause safety issues can also cause security issues

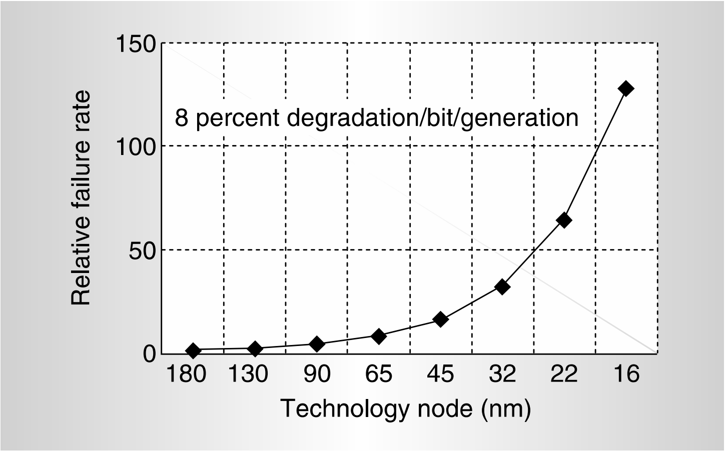
Fault Events

- ISO 26262 categorizes faults into Single-Point and Latent, and codifies metrics associated with probability and elapsed time.
- Being able to detect a certain number of faults, and quantify the hardware random failure rate determines the ISO 26262 safety level.
- Can security be compromised by these same events?
- Can an attack on a security component by detected the same way as a safety event?

Transient Faults



[Source: Baumann, 2005]

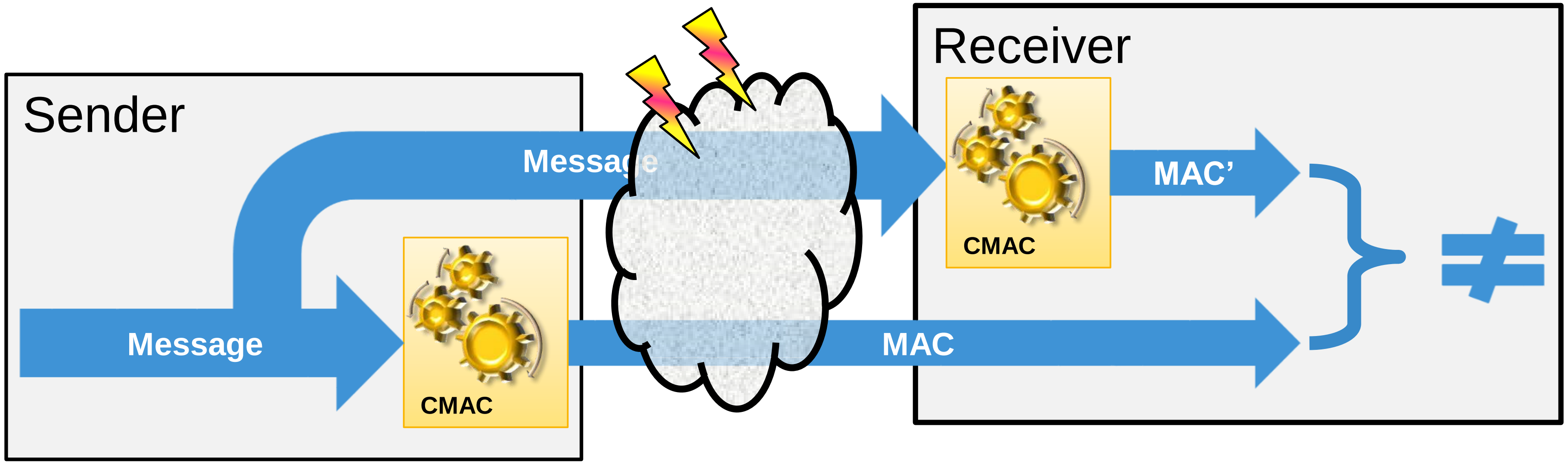


[Source: Borkar, 2005]

- Particle strikes upset transistors, causing glitches mistaken for real signals
- Repeated calculation corrects error
- From 180 nm to 16 nm, error rate increases >100x

Effect of Fault Events on Security (1 of 3)

- A side effect of good Cybersecurity systems and cryptographic algorithms is that they automatically detect the presence of a random physical fault condition.
- For example, the cryptographic algorithms used to authenticate and decrypt messages and data, automatically perform integrity checking
- If the data has been corrupted by, say by a random noise spike, the receiver of the data will know that has occurred

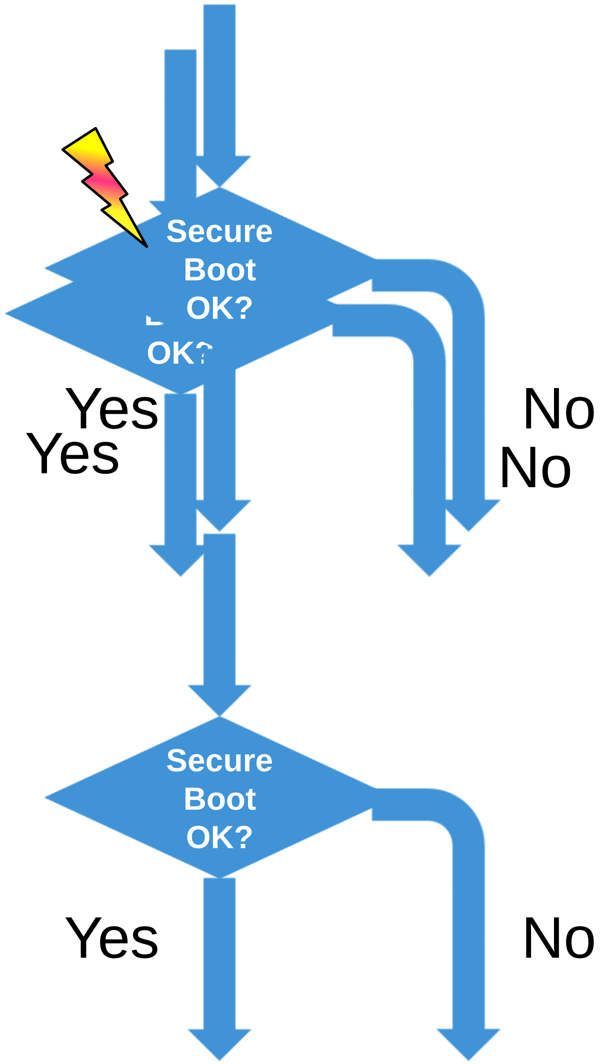


Effect of Fault Events on Security (2 of 3)

- A random noise spike on executing code may have a different effect. It could expose a security vulnerability
- However, if the system has been designed with functional safety in mind, a noise spike of this nature would be detected by the hardware, and corrective action taken
- If the noise spike were generated by a malicious actor (cyberspeak for bad person), the behavior of the hardware would be the same as for the random physical event
- So in this case, safety mechanisms provide the countermeasure to a security attack
- Now that’s cooperation!

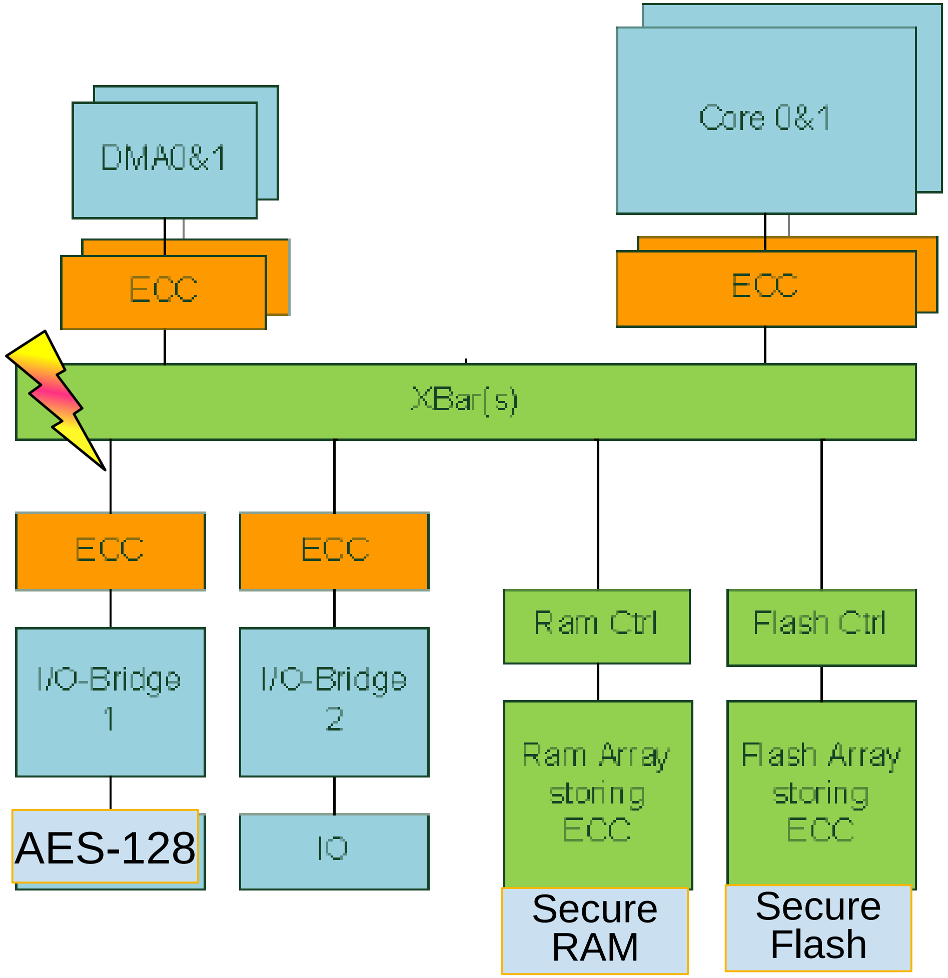
Security Fault Example 1 – Software Flow

- Trusted code execution flow may be compromised by a random or target attack.
- Setting status flags based on a corrupted test may cause a false positive or false negative.
- What is the impact of a false positive?
- Are false negatives safe?
- False results could be detected by:
  - Lockstep cores
  - Repeating the same test with random delay.
- Security is compatible with safety!



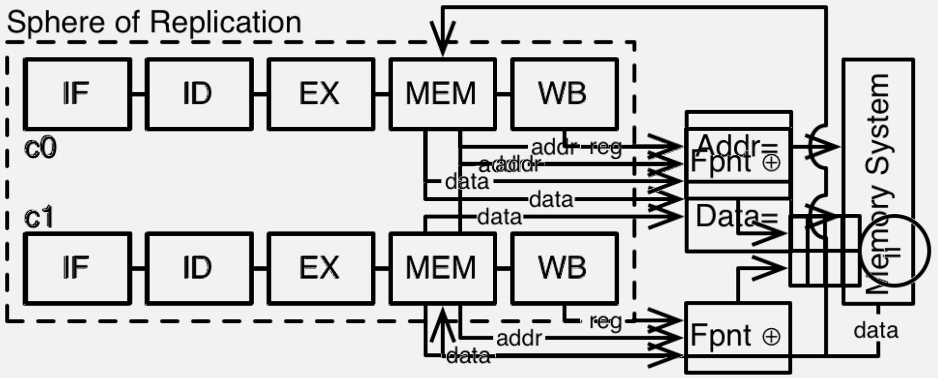
Security Fault Example 2 – Hardware Bus

- Trusted execution environment such as TrustZone
- Secure code executes through same safety hardware as application code
  - End-to-End ECC detects and corrects single bit errors on the bus
- Security is compatible with safety!



Execution Fingerprinting

- A typical fault tolerant lock step pipeline
- Adapted to perform Cryptographic hash function
- Provides fault detection of software threads
- Could satisfy fault coverage requirements for safety
- Not used as a security function, per se
- But can detect a side channel attack on code execution and data access
- A security function repurposed for safety



Fingerprinting system. Register values, addresses, and data are hashed; hashes are compared prior to committing a set of changes to the memory system.

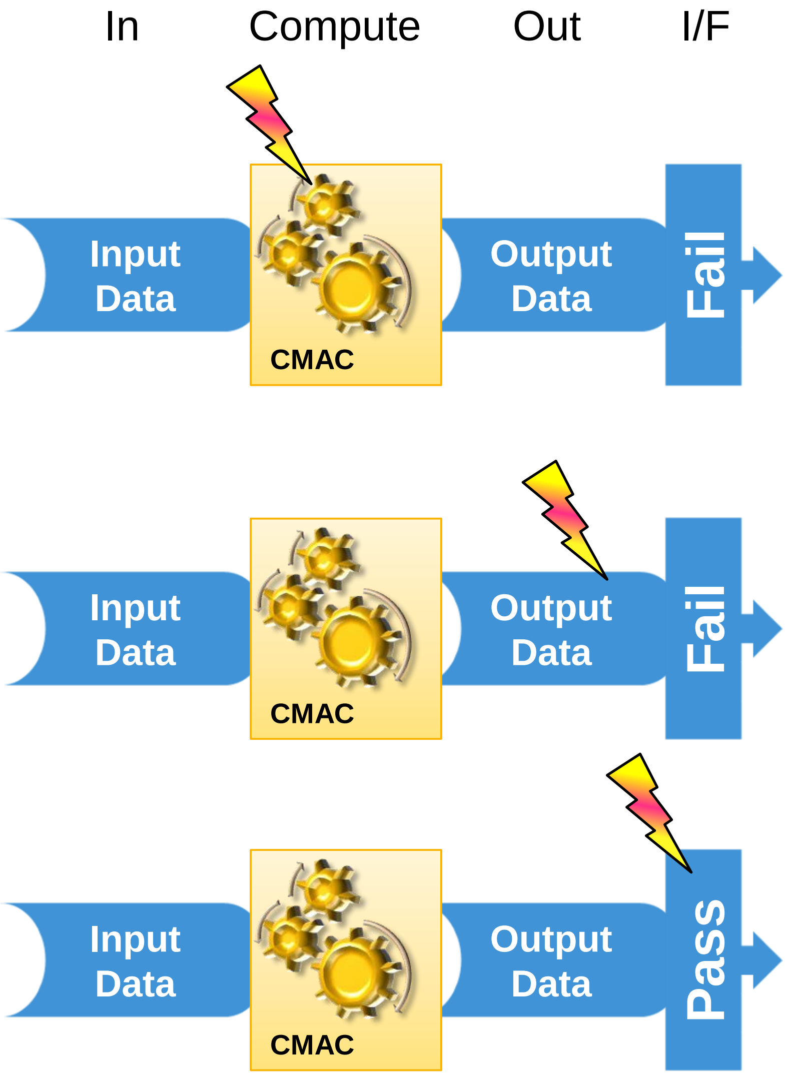
© 2014 Brett H. Meyer

Effect of Fault Events on Security (3 of 3)

- Most cybersecurity architectures contain a combination of both cryptographic functions and glue logic that provide interfaces with the rest of the system hardware
- Design decisions can be made by understanding the different impact of random physical events and malicious human intervention.
- For example, a cryptographic algorithm by itself will fail-safe, since corruption of data will result in detectable failure.
- However, the glue logic that returns the result of the algorithm may be connected through busses, memory and registers that themselves return a false positive result.

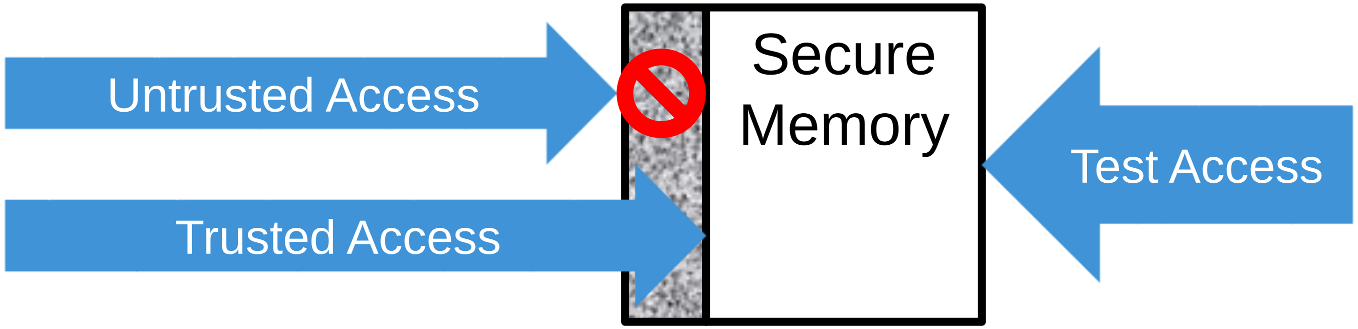
Security Fault Example 2

- Cryptographic function will fail on any random or targeted fault in the hardware directly involved in calculating the result, which could cause a false negative.
- Setting status flags based on the result of the cryptographic function may cause a false positive or false negative.
- What is the impact of a false positive?
- Are false negatives safe?



Test and Security Challenges

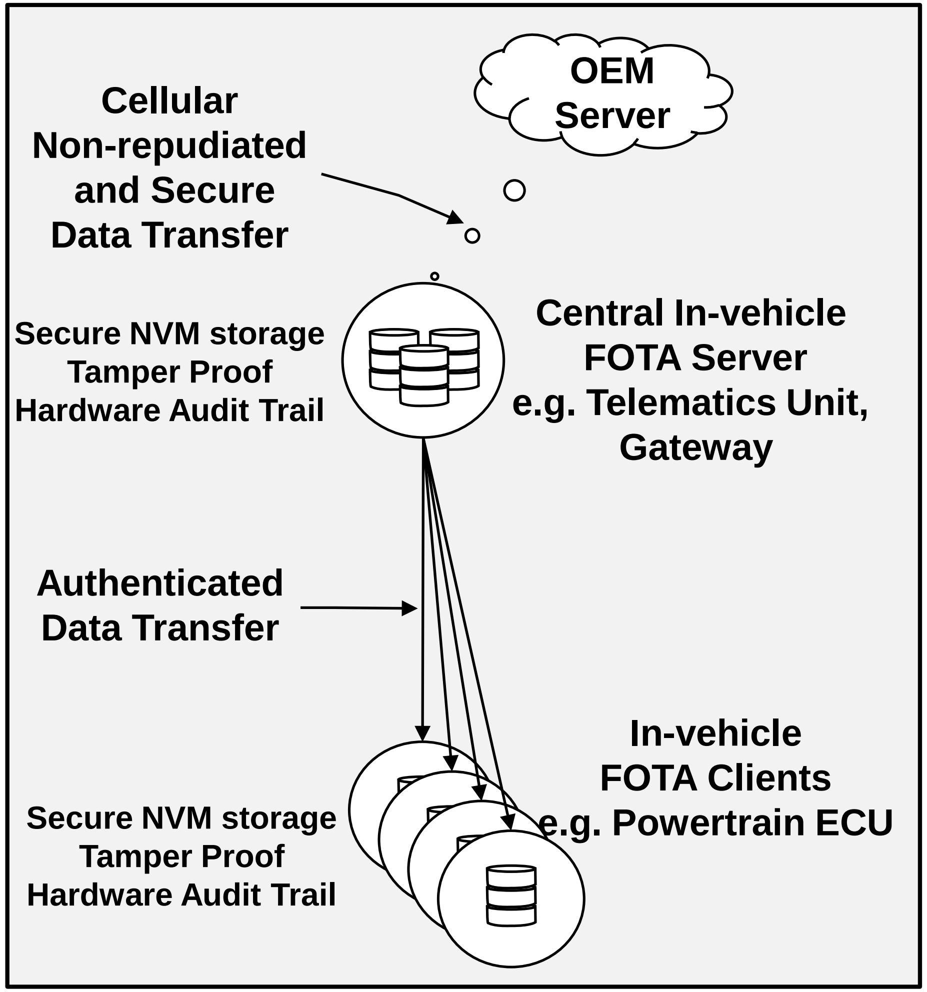
- Run time self test, or access to memory for Failure Analysis purposes poses interesting challenges for security.
- Self-test on RAM results in loss of any stored data.
- FA testing of RAM and NVM may allow unrestricted access to secure memory regions.
- This introduces a potential conflict of interests between safety and security.
- Careful system and test design can mitigate and even eliminate these conflicts.



Firmware Over The Air Update (Fota) Challenges

- Over the air updates offer many benefits
  - New features
  - Bug fixes
- Automobiles are cyber-physical devices
  - A bad FOTA update can have dangerous consequences
- A safe update requires end to end security
  - from OEM server
  - to embedded memory

§ Payment Card Industry


OEM Server
Cellular Non-repudiated and Secure Data Transfer
Secure NVM storage Tamper Proof Hardware Audit Trail
Central In-vehicle FOTA Server e.g. Telematics Unit, Gateway
Authenticated Data Transfer
In-vehicle FOTA Clients e.g. Powertrain ECU
Secure NVM storage Tamper Proof Hardware Audit Trail

Safety and Security Processes

Safety

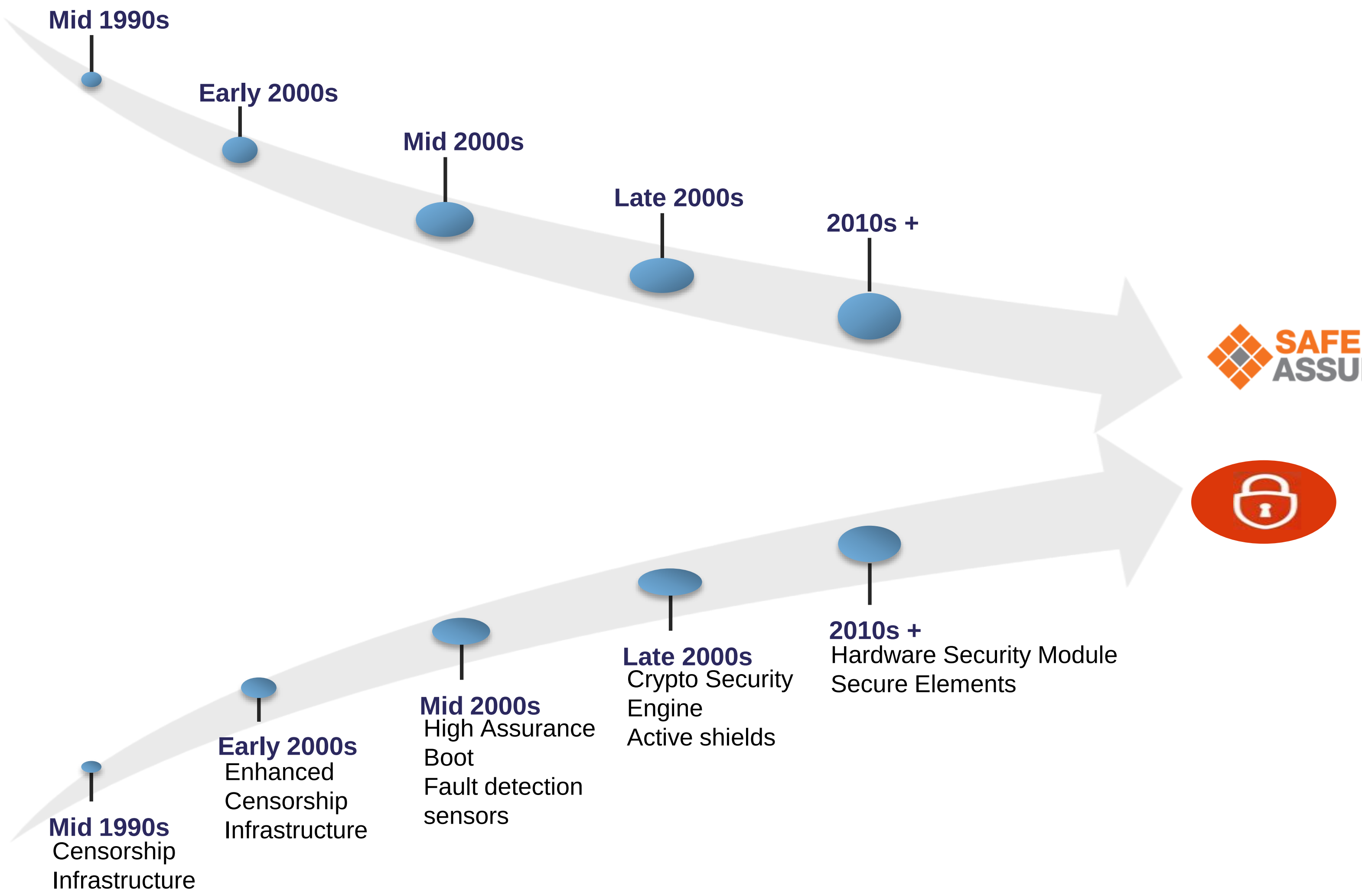
- ISO 26262
- Safety Goals
- Hazard Analysis
- Risk Assessment
- Safety Concept
- FMEDA, FTA
- FTTI (Fault Tolerant Time Interval)
- Safety Manual

Security

- DREAD
- Security Goals
- Attack Surfaces
- Threat Model
  - Use cases, entry points, assets, data flow
  - Rank Threats, Countermeasures
- Standards?

Safety+Security?
DO-236/A

The Meeting of Safety and Security Domain Expertise



Mid 1990s

Early 2000s

Mid 2000s

Late 2000s

2010s +

SAFE ASSURE™

Mid 1990s
Censorship
Infrastructure

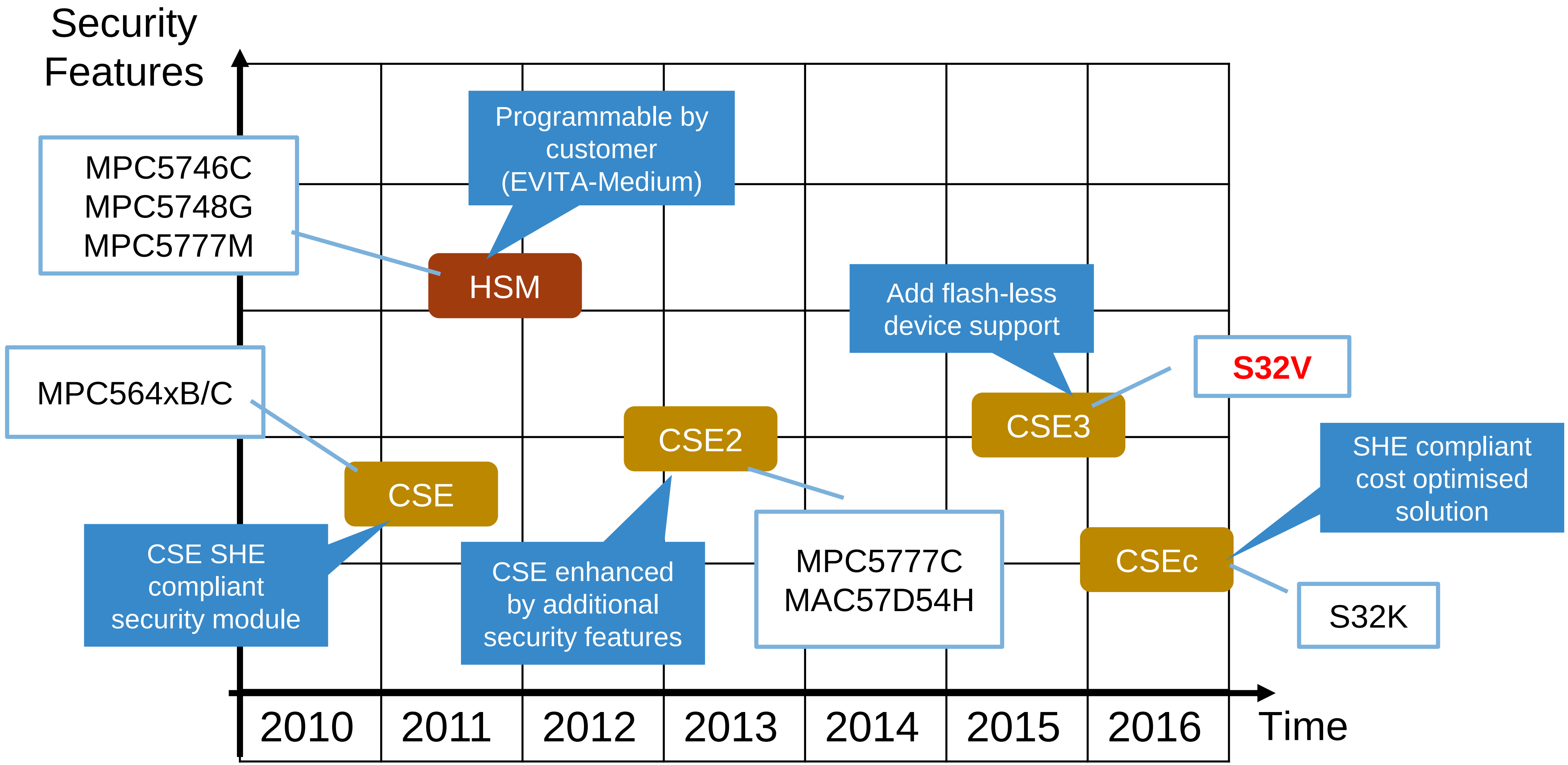
Early 2000s
Enhanced
Censorship
Infrastructure

Mid 2000s
High Assurance
Boot
Fault detection
sensors

Late 2000s
Crypto Security
Engine
Active shields

2010s +
Hardware Security Module
Secure Elements

S32 NXP Security Modules


Security Features
MPC5746C
MPC5748G
MPC5777M
Programmable by customer (EVITA-Medium)
HSM
MPC564xB/C
Add flash-less device support
S32V
CSE3
CSE2
CSE
SHE compliant cost optimised solution
CSE SHE compliant security module
CSE enhanced by additional security features
MPC5777C
MAC57D54H
CSEc
S32K
2010
2011
2012
2013
2014
2015
2016
Time

THANK YOU

SECURE CONNECTIONS
FOR A SMARTER WORLD

ATTRIBUTION STATEMENT