UNIMORE
UNIVERSITÀ DEGLI STUDI DI
MODENA E REGGIO EMILIA

Dipartimento di Ingegneria
"Enzo Ferrari"

Automotive Cyber Security

Lecture 2 – A bird's-eye view of automotive cyber defenses

Mirco Marchetti

Università di Modena e Reggio Emilia

mirco.marchetti@unimore.it

How to “secure” something?

Option 1: make it invulnerable to any kind of attack. Impossible.

Option 2: try to “raise the bar” for the attacker.
A secure system is not an invulnerable system. It is a system that is so difficult to violate that attackers fail or desist.

- “Limited” attackers cannot violate it
- Resourceful attackers prefer to attack easier targets

Same concept in cyber and physical worlds
https://www.ferrarini.pr.it/https-www-ferrarini-pr-it-classi-sicurezza-antieffrazione/

Software vulnerabilities will be there

- **Software vulnerability:** simply put, it is a bug that allows an attacker to violate confidentiality, integrity or availability
  - Users may not even realize that the system is vulnerable, maybe they just complain about a bad user experience
  - Attackers like bugs! Because some of these bug allow them to expose confidential data or to deviate from the instruction flow defined by the programmer
- By exploiting a vulnerability an attacker can accomplish many tasks, usually attackers go for arbitrary code execution

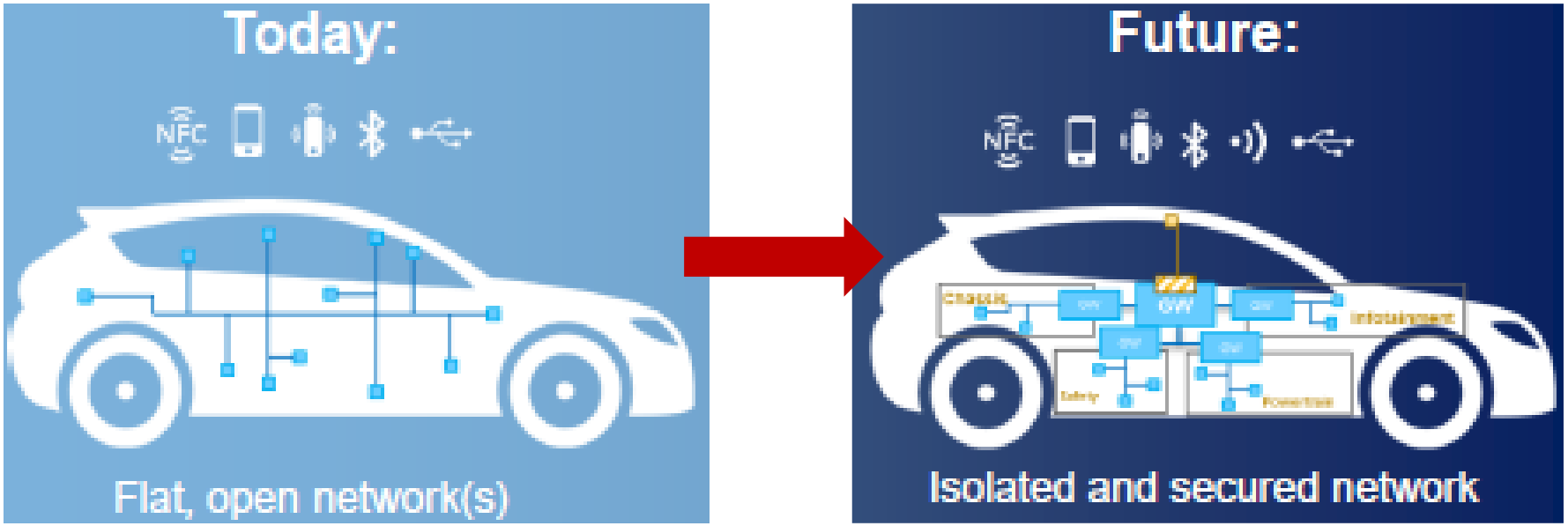
Lessons learned from IT (1)

- **In modern IT security the concept of *Perimeter Security* is seen as nonsense**. Once attackers have breached perimeter boundaries, it is easy to move laterally among connected nodes

- Solutions
  - ➔ **Avoid Candy-Coated Security**: *crunchy* on the outside, *gooey* on the inside
  - ➔ Need security (especially **Authentication**) even on internal networks, ECUs, processes, firmware/software updates
  - ➔ Need Intrusion **Detection** to give awareness
  - ➔ Need Intrusion **Prevention** or at least some automatic mitigation to enable **timely** responses

Defense-in-depth

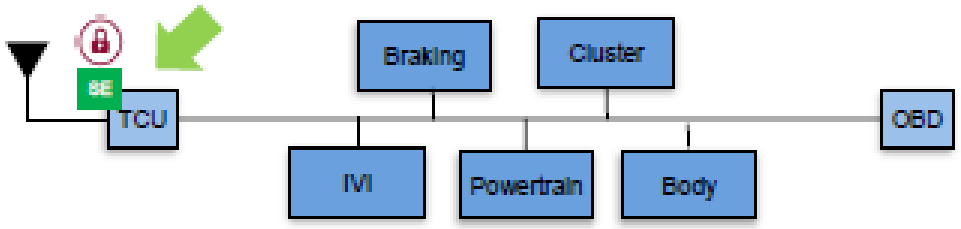
Multiple layers of protection, at different levels to mitigate the risk of one component of the defense being compromised or circumvented



Multi-layer security - *network*

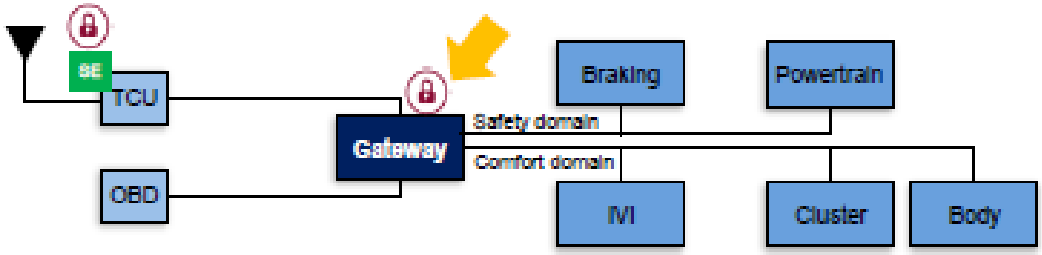
Layer 1: Protect External Interface

Secure M2M authentication, secure key storage



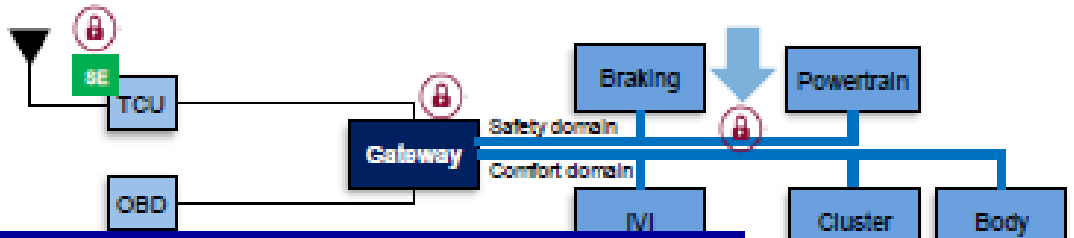
Layer 2: Isolate Network

Domain isolation, firewall/filter, centralized intrusion detection (IDS)

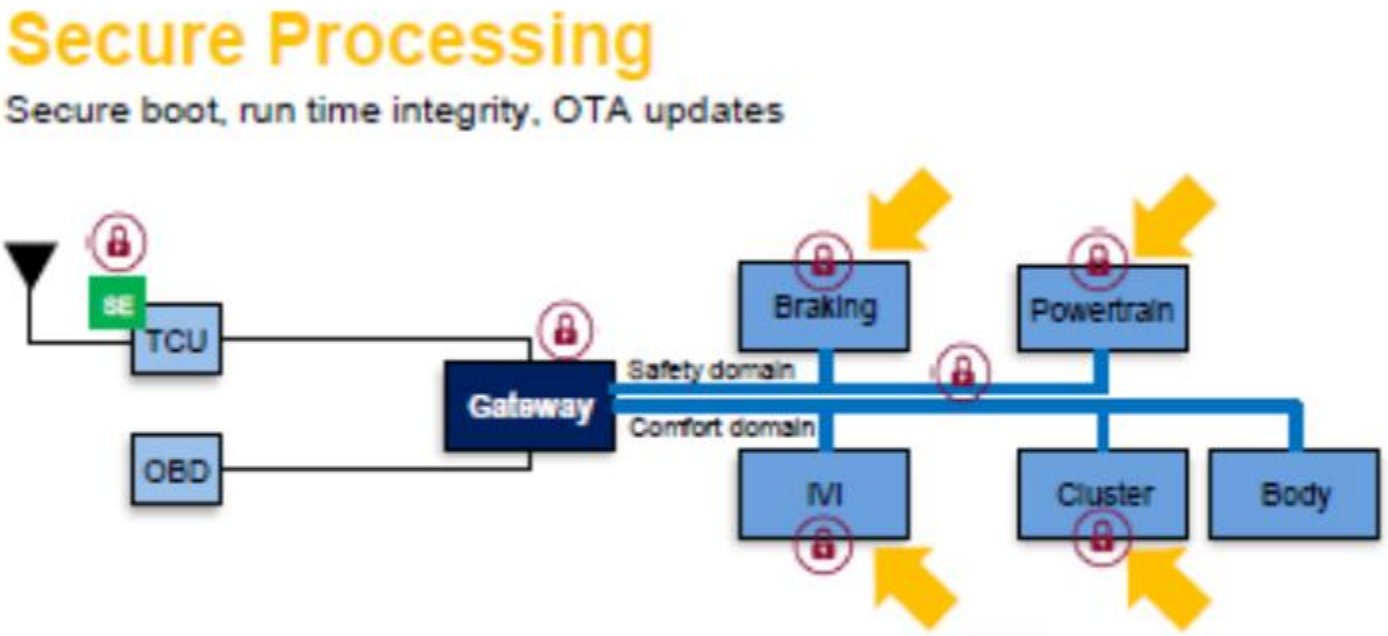


Layer 3: Secure Network

Message filtering, message authentication, distributed intrusion detection (IDS)



Multi-layer security - *processing*



Security during the entire life time

- State-of-the-Art-Security when produced …, but once the vehicle is in operation the attack landscape continuously changes:
  - Pen Testers find new vulnerabilities
  - Attackers develop new cyber attacks
  - Vehicles evolve at firmware and software levels
  - New connected services create new attack vectors
  - Cars are dismantled, ECUs can be bought as spare parts. What about their data?
- **How can we ensure that vehicles remain protected through their entire lifetime (*much longer than a typical IT product*)?**

Vehicle scenarios are different from IT

- Device-centric M2M, not user-centric scenario
- Real-time environment
- Long lifecycle of devices (5-40 years)
- Not all devices are permanently connected
- Constraints for bandwidth, storage, processing

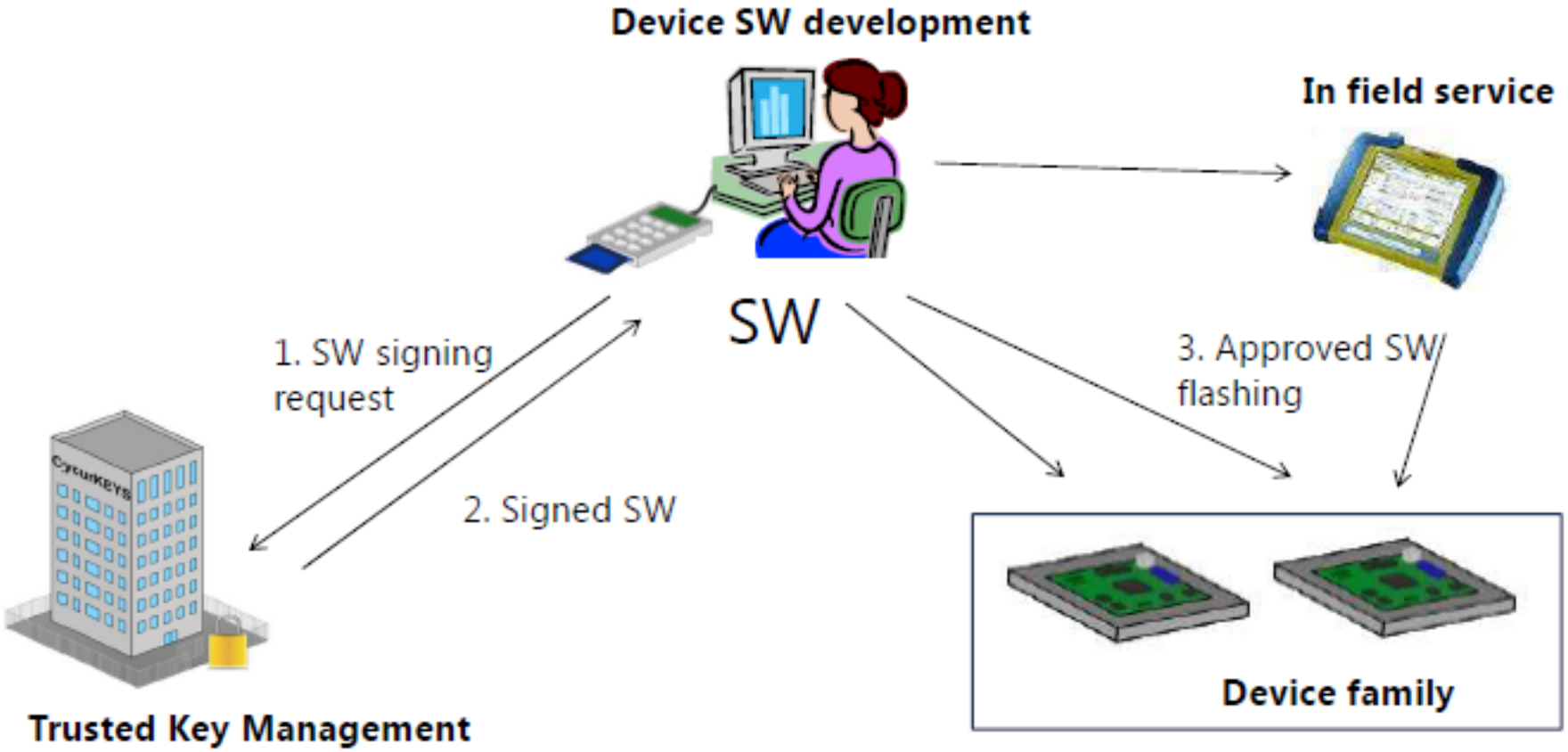
  - Classical IT data formats (e.g., X.509) are not suitable for all communications
  - Symmetric *vs* Asymmetric Key management systems?
  - RSA *vs* Elliptic Curve Cryptography?
  - Key and Certificate Infrastructure for embedded systems?

Securing a car: *Remediation*

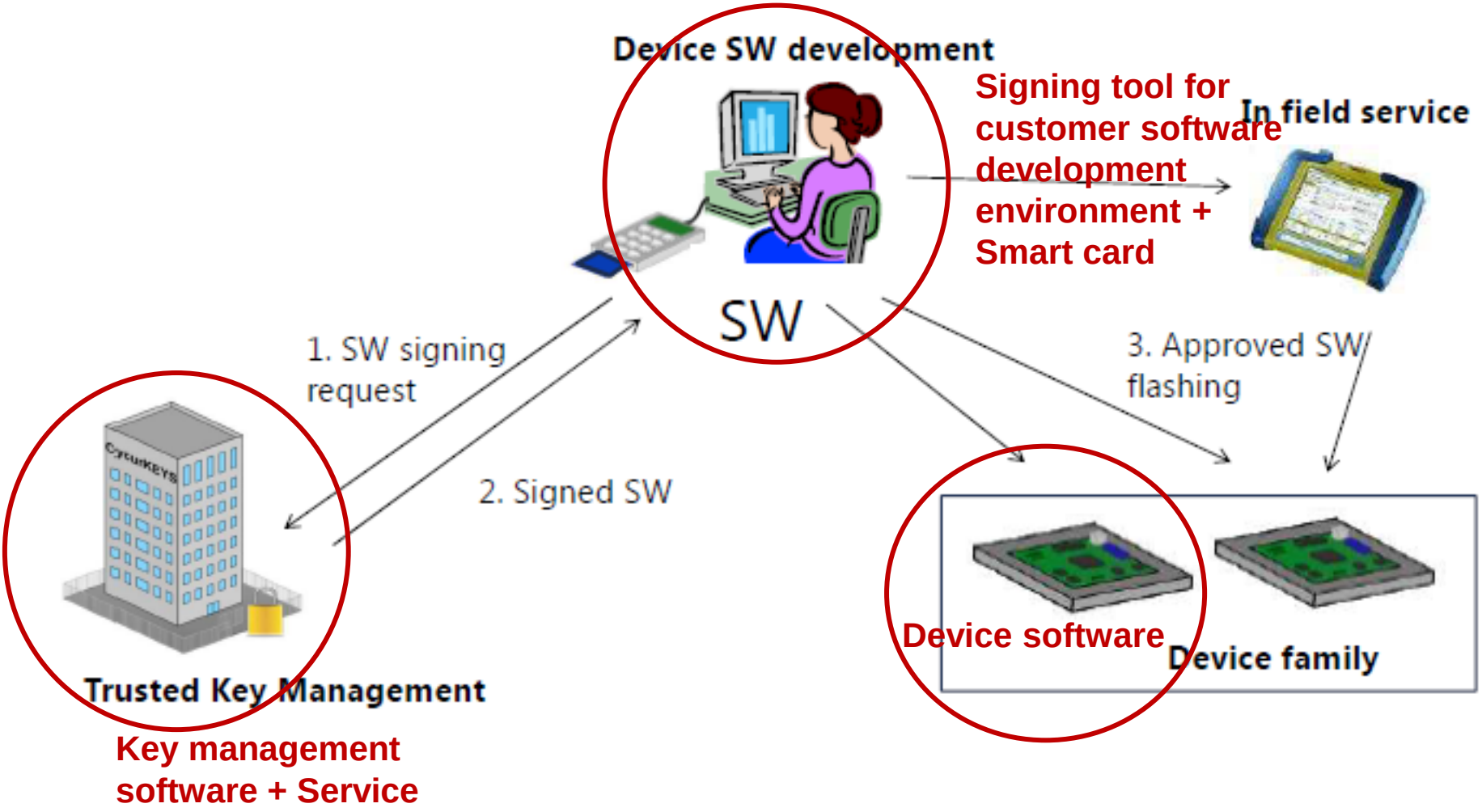
- **Secure FOTA is key enabler for response**
  - Immediate reaction becomes possible without large-scale recalls
  - Holistic FOTA security approach

- **Secure FOTA requires end-to-end security mechanisms**
  - Authenticity
  - Integrity
  - Confidentiality (optional)

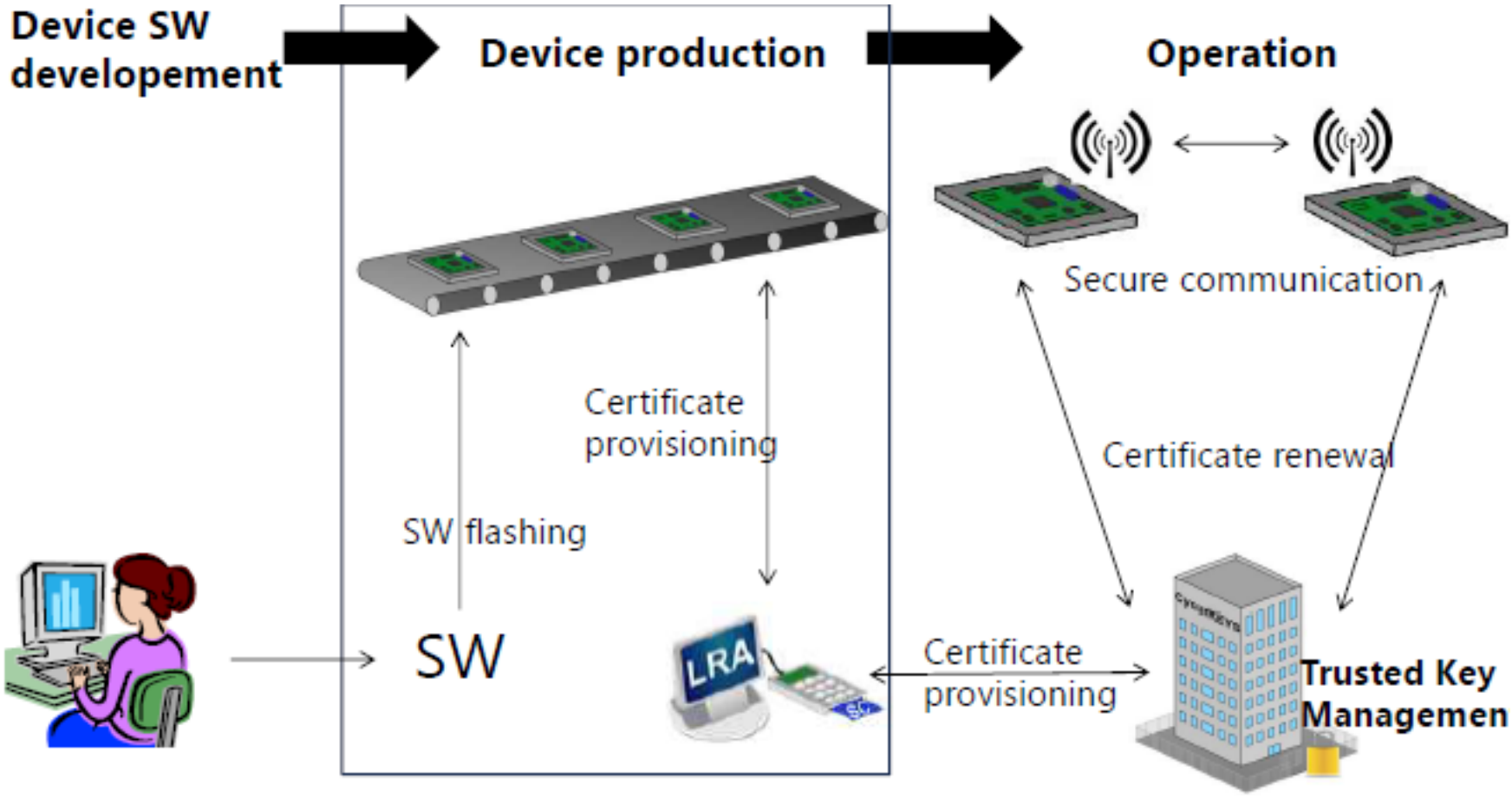
Securing software update
(from authorized developers only)



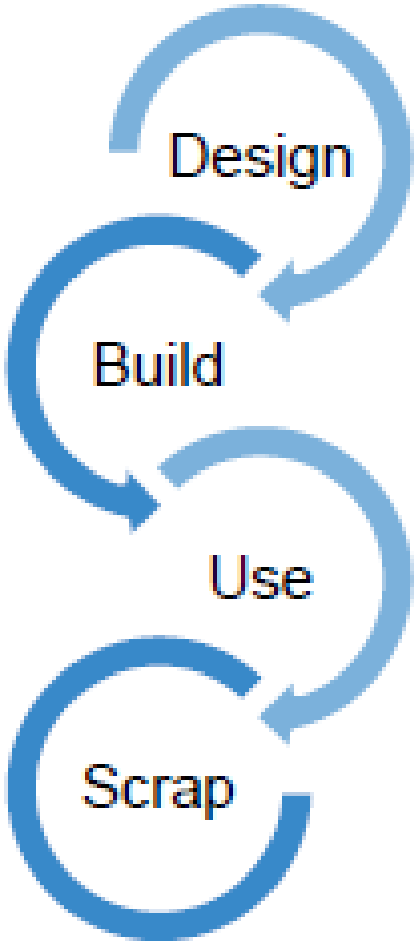
Securing software update
(from authorized developers only)



Securing the communication of devices (V2V)



Security processes and services



- Requirement specification
- Architecture design
- Detailed design

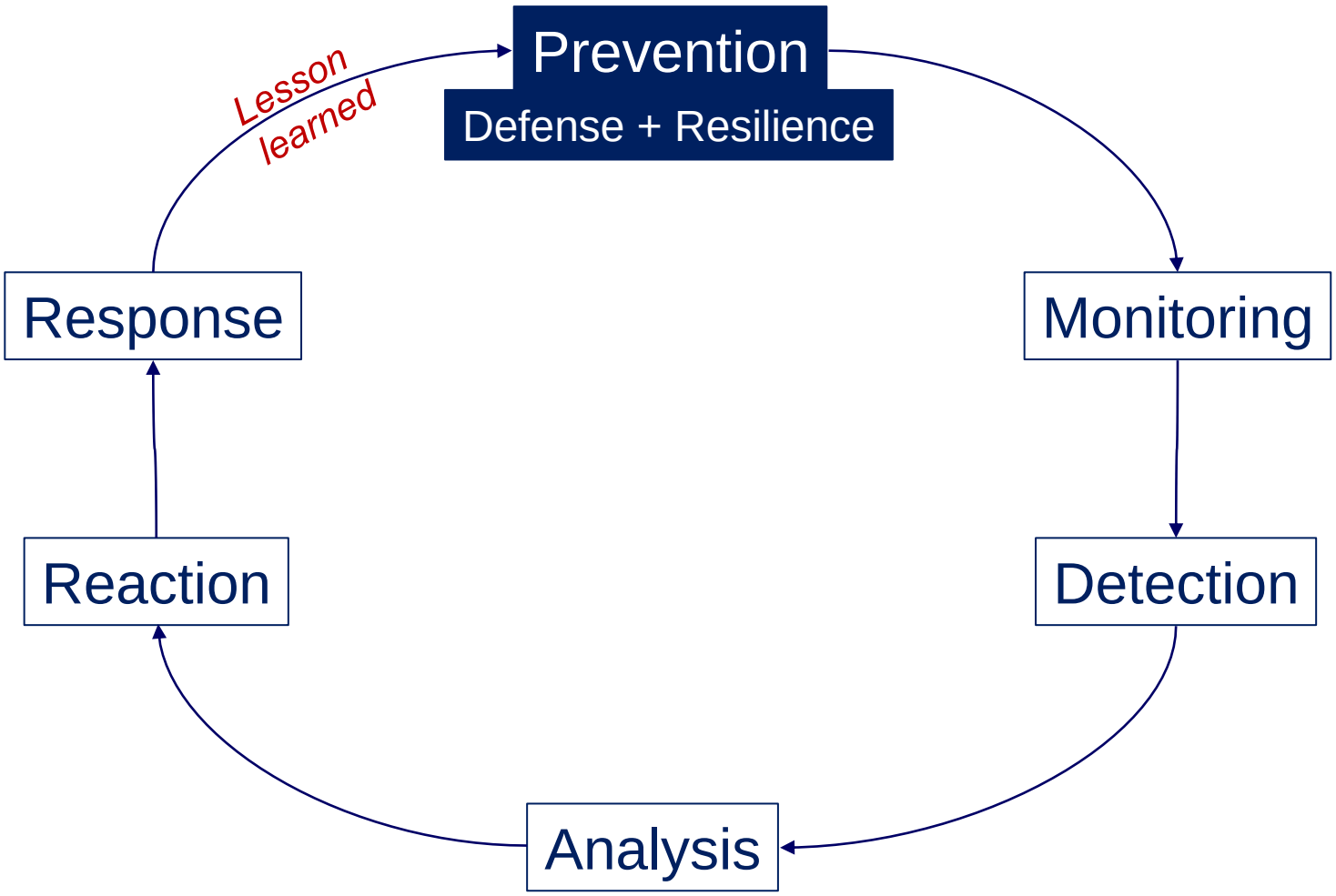
- Implementation
- Validation & Verification

- Maintenance (FOTA)
- Upgrades (Feature unlock)

- Failure analysis
- Decommissioning

Overall view to security

Cyber defense cycle



Post-prevention

1. Continuous monitoring of attacks in the field
2. Timely detection of attacks
3. On-line analysis
4. Immediate reaction

ON-LINE

5. Offline analysis, including forensics by experts
6. Response, e.g., roll-out of countermeasures through updates for the entire fleet

OFF-LINE

1. Monitoring

- Need to monitor both network communications and activities within ECUs
- The Network IDS (intrusion detection system) module can either be integrated into a central ECU with access to all communications, or multiple IDS modules can be integrated into multiple ECUs depending on the vehicle architecture

- The Host IDS module has to be implemented in (ideally) all ECUs. At least in the safety relevant ones

2. Detection

- A vehicle is manufactured with a known set of ECUs and related messages, usually documented within a DBC file
- Based on this information, a set of detection rules can be created that reflects the target vehicle architecture

NOT SO EASY, as we will see…

3. Analysis

- Once an anomaly is detected, there is a typical triage phase
  - Real attack or false positive?
  - Type of anomaly
  - Severity

4. Immediate reaction

- Depending on attack, activate countermeasures
  - on the CAN bus
  - on some ECU
  - on the car behavior
  - …

It is still an open issue!

Post-prevention

1. Continuous monitoring of attacks in the field
2. Timely detection of attacks
3. On-line analysis
4. Immediate reaction

ON-LINE

5. Offline analysis, including forensics by experts
6. Response, e.g., roll-out of countermeasures through updates for the entire fleet

OFF-LINE

5-6. Off-line analysis, response and forensics

- Store the detected anomaly and record context data
- Send to backend to be analyzed by experts → recently **Product Security Incident Response Team** (PSIRT) for vulnerability handling:
  - Internal/External Interface for Researchers
  - Handle the disclosure requirements
  - Advisory-Service
  - Security Community involvement
  - Social Community Monitoring
  - Incident Handling
- Forensics is mandatory in case of incident, casualty, victim
- **Insurance black-boxes are not yet equipped with component suitable to Court Criminal Procedures!**

PSIRT

- The single point of contact when external parties want to disclose/discuss vulnerabilities in company products
- It ensures that vulnerability claims are resolved timely and according to their criticality together with development groups
- It assists business units to understand vulnerabilities technically, but also to communicate appropriately with outside entities, and to navigate within the complexity of the security ecosystem
- The PSIRT should be the most trusted vulnerability and product security information source, both for parties from outside but equally from inside the company

Disclosure

- **Coordinated disclosure:** An external party notifies the PSIRT some time before publication
  - The party collaborates
  - The vulnerability stays confidential until the Company has a fix

- **Uncoordinated disclosure:** An external party immediately discloses a vulnerability to the public (e.g., via internet or at a conference) without vendor pre-notification

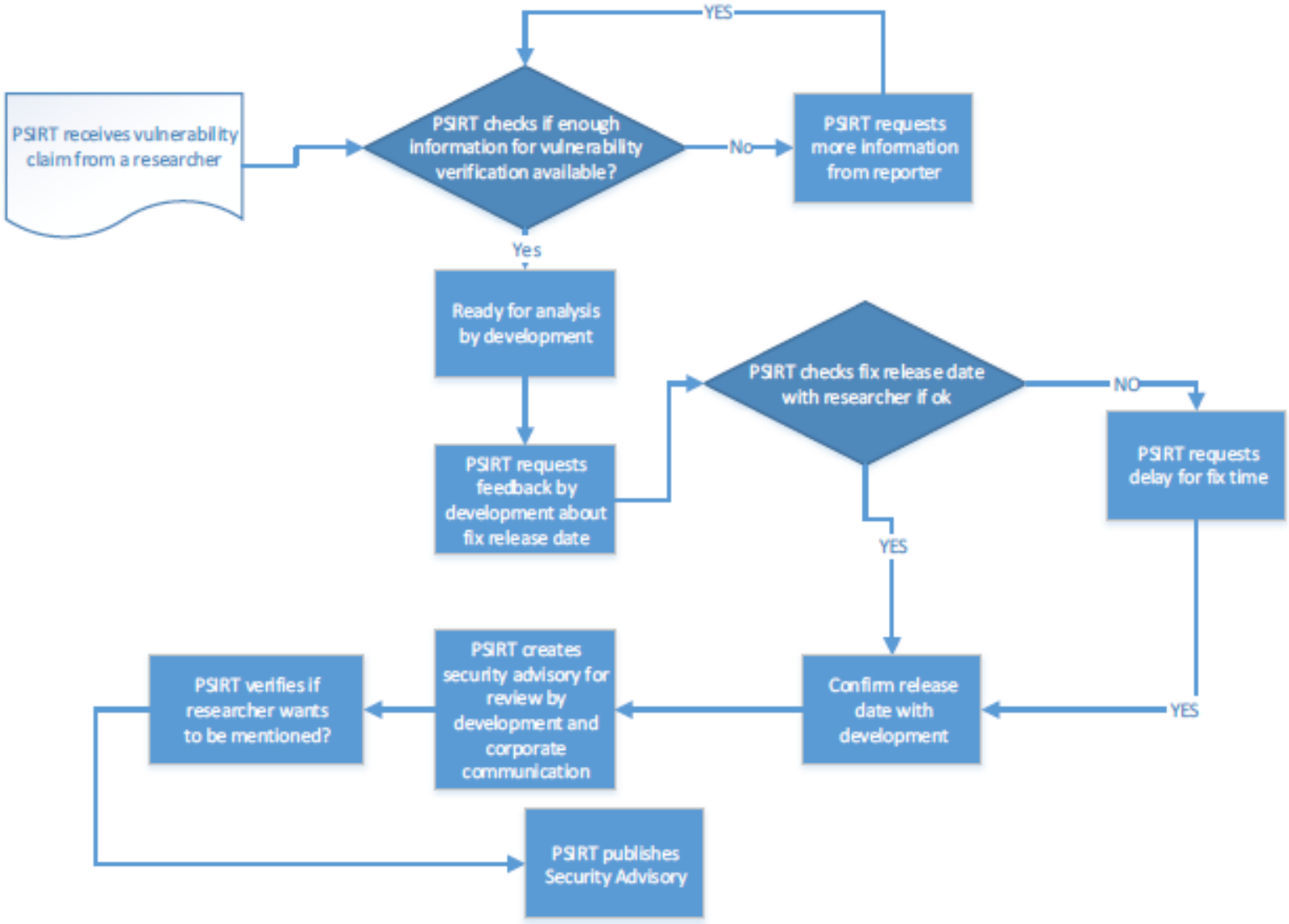
  ➔ Holding-Statement is needed
  (https://useworkshop.com/blog/11-examples-of-holding-statements/)

Be ready to both!

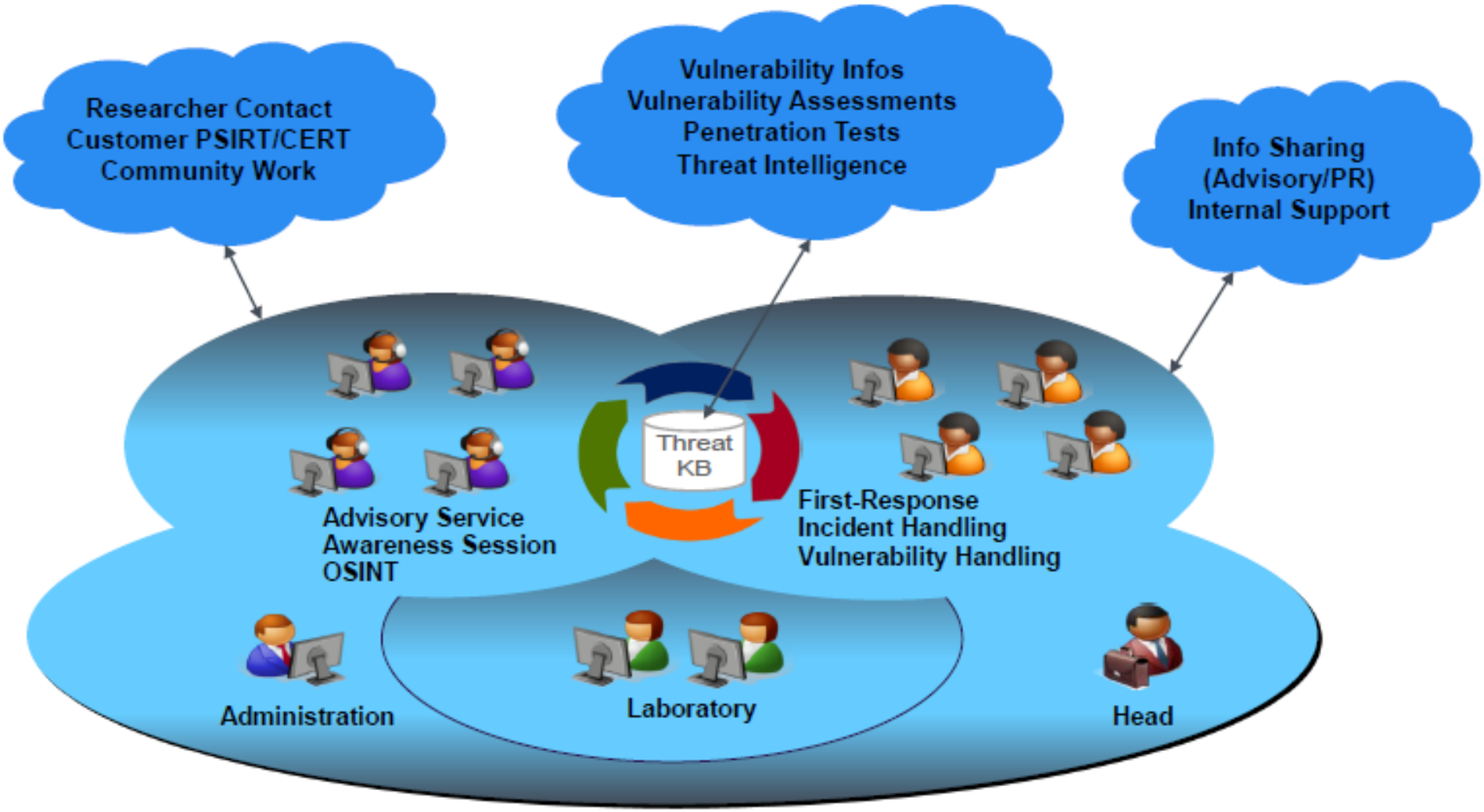
Coordinated disclosure management

1. **Awareness**: PSIRT receives notification of security incident
2. **Active Management**: PSIRT prioritizes and identifies resources
3. **Fix Determined**: PSIRT coordinates fix and impact assessment
4. **Communication Plan**: PSIRT sets timeframe and notification format
5. **Integration and Mitigation**: PSIRT engages experts and executives to create patches to harden the affected ECUs, and to send upgrade to the entire fleet of vehicles
6. **Notification**: PSIRT notifies all customers simultaneously
7. **Feedback**: PSIRT incorporates feedback from customers and internal input

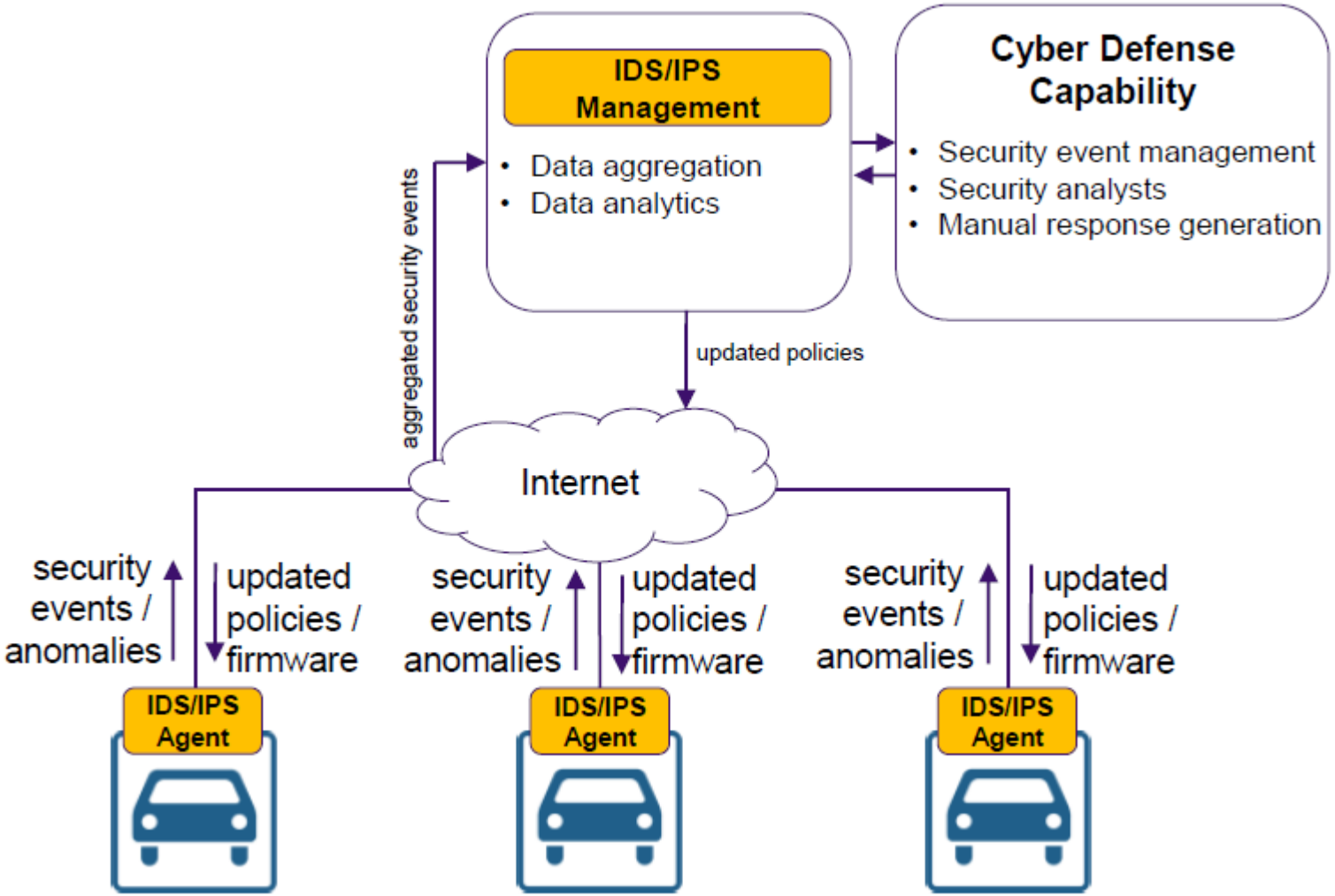
Vulnerability handling process



Pro-active PSIRT



Integrated defensive system

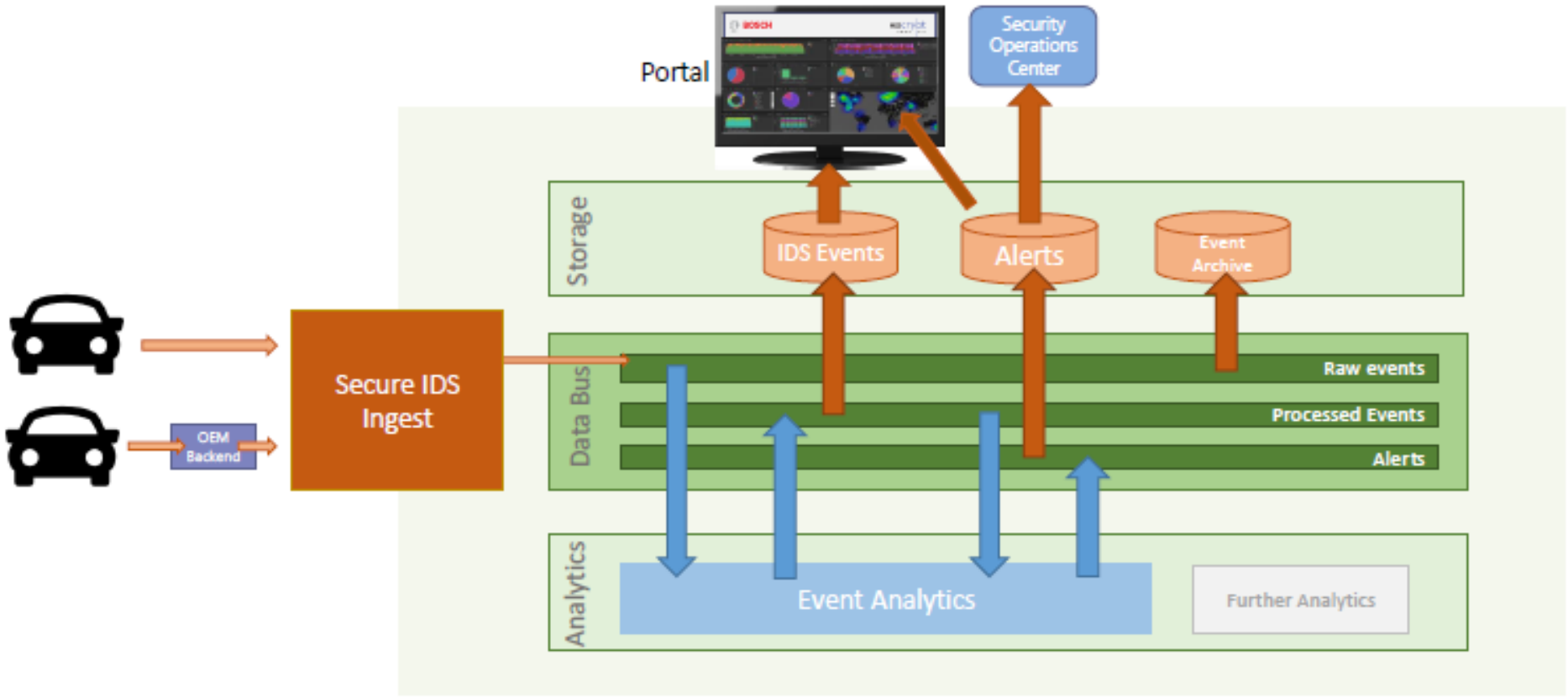


Car connection

- Not all cars are going to be *always connected*, and connectivity takes many forms: from a car fully connected 24/7 to one that is only connected during scheduled maintenance or troubleshooting
- Nevertheless, researchers should look to the future:
  - Data that comes in periodically is still valuable information that can be analyzed to help informed decisions
  - Connectivity will improve over time, so it is important to lay the groundwork now and build the tools along the way, while realizing the immediate benefits

Analytics on-Cloud

- Embedded systems have limited storage capacity, and connectivity is not yet ubiquitous, making the storage of IDS events expensive
- The more data the in-car IDS can send to the back-end infrastructure, the more can be analyzed. Identify important data and guide deployment to maximize “immunity response”
- Without a way to investigate, evaluate, and analyze the data coming from the embedded IDS, the operational value of in-car IDS is minimal. Deploying a strong system is important, and in other industries back-end systems have proven to be very effective in providing security, intelligence and response (e.g., credit card systems)


Portal
Security Operations Center
Storage
IDS Events
Alerts
Event Archive
Data Bus
Raw events
Processed Events
Alerts
Analytics
Event Analytics
Further Analytics
Secure IDS Ingest
OEM Backend

- Detect and respond in real-time to ongoing cyber security attacks
- Overview the cyber security of the entire vehicle fleet
- Focus cyber security strategy and implementation, provide cost efficiencies
- Fulfill government cyber-security recommendations and (future) legal requirements
- Avoid potential cyber-security recalls with timely incident response
- Avoid expensive manual ECU updates to address cybersecurity issues
- Improve customer confidence and manufacturer image and reputation

Risks of data outsourcing

- Passive attackers do not modify data, but can:
  - sell data to competitors
  - leaked data publicly
  - loose data (e.g., theft of hard drives)

- Active attackers can:
  - modify and corrupt data
  - delete data
  - generate fake data
  - generate incorrect results

Problem: how to leverage benefits of data outsourcing while providing confidentiality and integrity guarantees?

In summary

- Anything connected is going to be attacked
- At the very lest, some **in-car security solutions**
- To ensure millions of connected cars are secure over their entire lifetime, you need a way to gather, analyze, and act upon the data from the in-car devices (e.g., firewall, IDS, sensors) to some on-cloud solutions → permanent connection + cloud + big data analytics