# Connected Vehicle Cybersecurity Volvo Group Trucks Technology


**Christian Sandberg, Volvo GTT**
**Presentation material:**
**Andreas Bokesand, Christian Sandberg**

**Chalmers, DAT300, 2019-10-21**

# WannaCry Ransomware Attack 2017-05-12


230 000 computers in 150 countries affected

- British Hospitals severely impacted
- Maersk reported financial impact 250M$
- ...

Imaginary – not a real case!

# Your car ?

## - impacting your ability to travel



http://virusguides.com/wp-content/uploads/2016/09/ransomware-attacks-cars.jpg
https://www.intelligentenvironments.com/wp-content/uploads/2016/11/Ransomware-Car.png

# Trucks ?

## - Impacting transportation of goods!

**In the first 24 hours…**

- Hospitals will run out of necessary supplies.
- Service stations will begin to run out of fuel.
- Just-in-time manufacturing get component shortages.

**In just 2-3 days…**

- Food shortages, consumer hoarding and panic.
- Garbage will start piling up in urban areas.
- Container ships will sit idle in ports and rail transport will be disrupted

**In just one week…**

- Automobile travel will cease due to lack of fuel.

(US-centric scenario)

https://www.tdsource.com/2016/08/03/if-trucking-stops

# Volvo Group - What we do

We are one of the world's leading manufacturers of **trucks, buses, construction equipment and marine and industrial engines**.

**ON THE ROAD**
Our products help ensure that people have food on the table, can travel to their destination and roads to drive on.

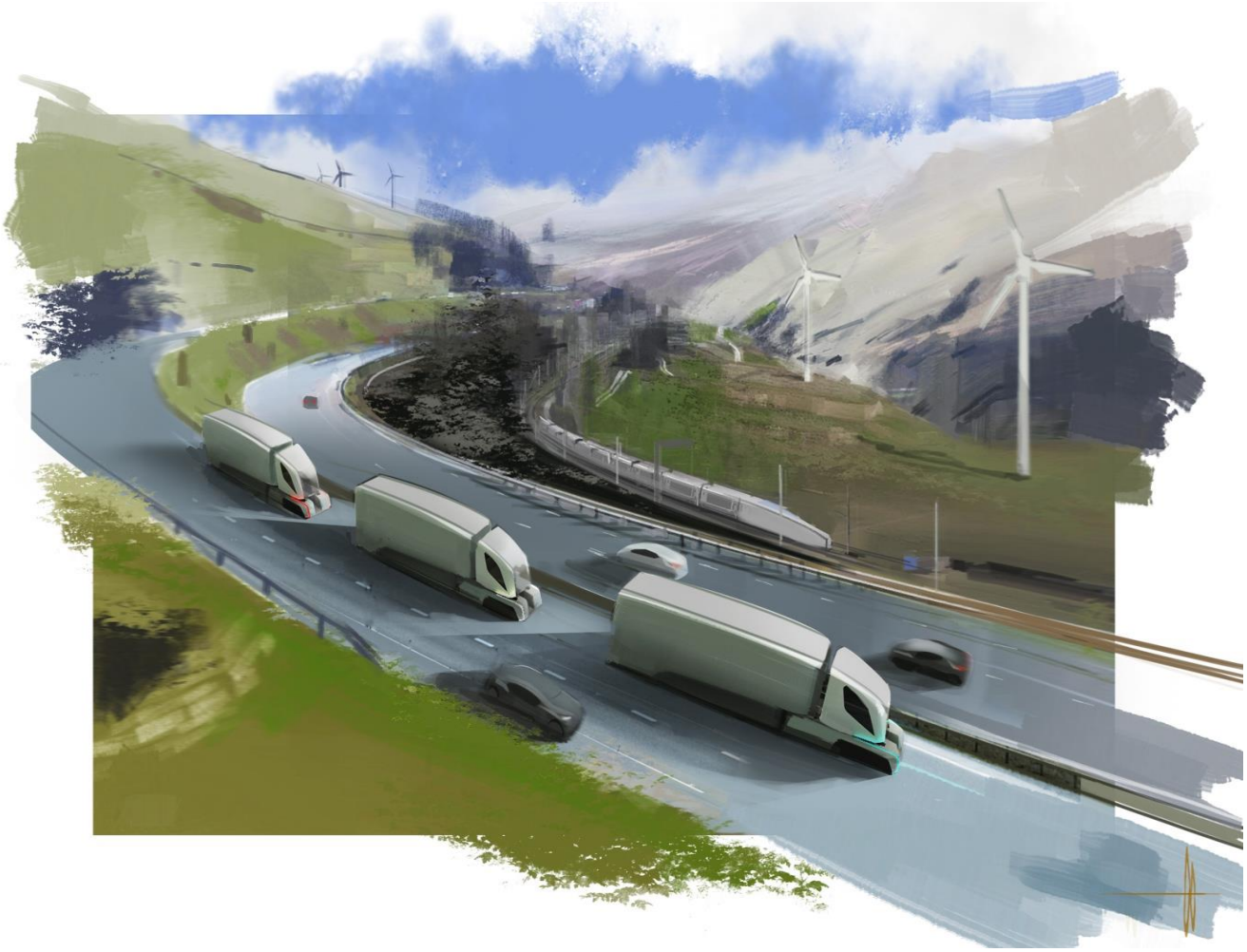
**IN THE CITY**
Our products are part of the daily life. They take people to work, distribute goods and collect rubbish. We are developing tomorrow's public transport solutions.

**AT THE SITE**
We contribute to the extraction of some of the world's most important raw materials. Our engines, machines and vehicles can be found at mining and construction sites and in the middle of forests.

**AT SEA**
Our products and services are with you, regardless of whether you are at work on a ship or on holiday in your pleasure boat.

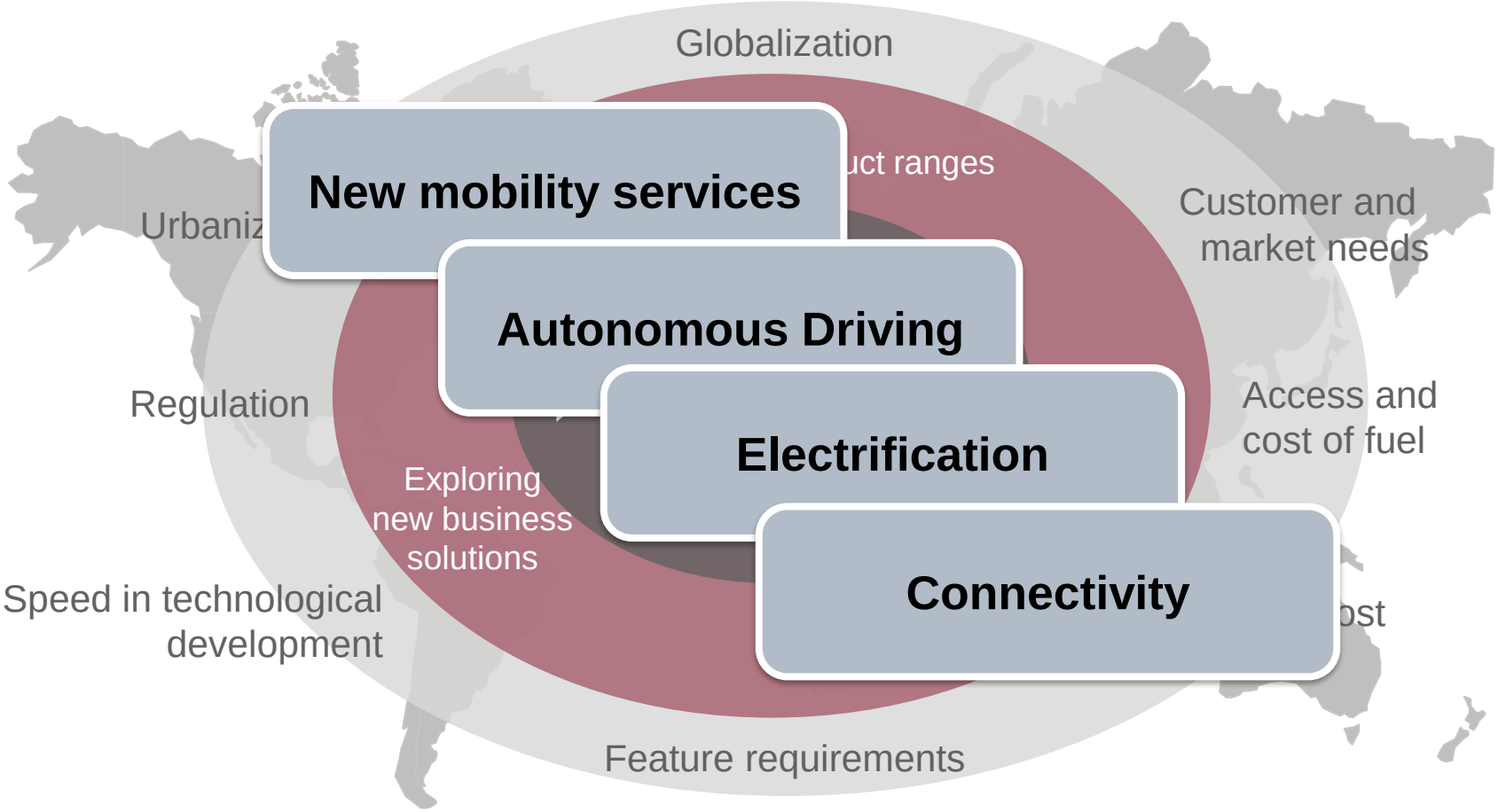
# Group Trucks Technology

Our organization for **research and product development** of complete vehicles, powertrain, components and service offering.



# The World Evolve

## - Drivers for new technology



# The classic vehicle

## ... was a self-contained system

# The modern vehicle

## ... is essentially a full IT infrastructure, on wheels!

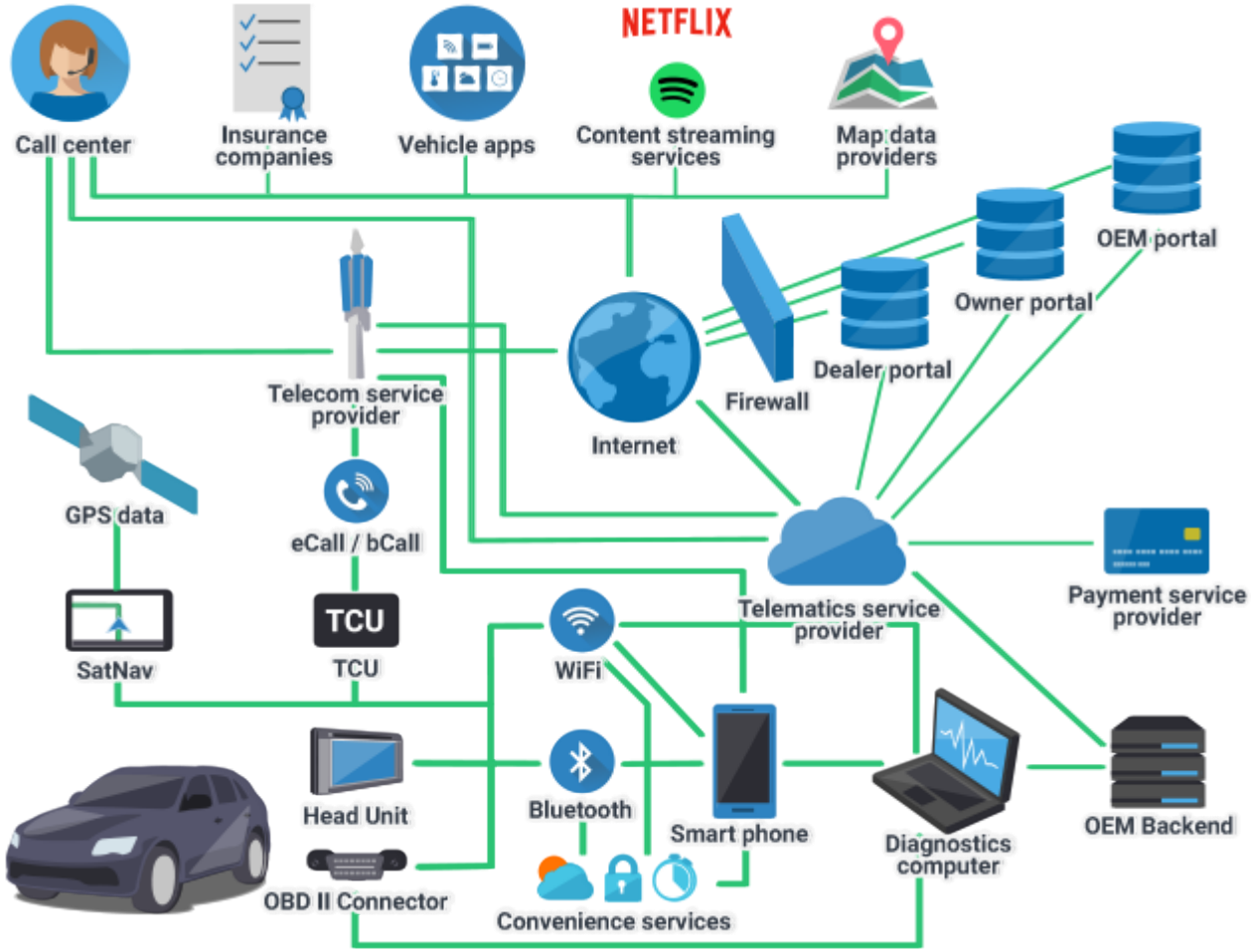

http://www.starhub.com/content/dam/starhub/2016/business/resources/blog/mobile-security-breaches-you-need-to-prevent-today/content-image-unsecured-network.jpg

# The future vehicle

## ... is autonomous, electric and computationally powerful

# Connected vehicles

## - The more things are connected, the higher the security concern



# Researchers demonstrate the potential

**July 21, 2015: "Hackers remotely kill a Jeep on the highway"**
**Source:** http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
**Details:** http://illmatics.com/Remote%20Car%20Hacking.pdf

**Feb 24, 2016: "Nissan Leaf easily hacked through browser-based attacks"**
**Source:** http://www.bbc.com/news/technology-35642749/
**Details**:http://www.troyhunt.com/2016/02/controlling-vehicle-features-of-nissan.html

**Sep 20, 2016: "Researchers remotely hack Tesla Model S"**
**Source:** https://www.washingtonpost.com/news/the-switch/wp/2016/09/20/researchers-remotely-hack-tesla-model-s/

**Aug 2, 2016: "Hackers hijack big rig truck's accelerator and brakes"**

**Source:** https://www.wired.com/2016/08/researchers-hack-big-rig-truck-hijack-accelerator-brakes/

# Attackers and Motivations

**Researcher** may want to showcase and increase awareness

**Authorities** may require functionality for law enforcement, **owner** want to circumvent

**Hacker** wants Fun, Fame

**Driver** want higher road speed limit, **owner** want to control fuel consumption

**Third party** developers want to offer add-ons and tuning

**Fleet/Vehicle owners** may want to “upgrade” their own vehicles

**Criminal** wants to disable vehicle to steal goods

**Thief** wants to disable alarm or immobilizer, copy/add keys

**Competitor** can be interested in intellectual property

**Criminals** can earn money by vehicle ransom

# Attackers and Attack vectors

**Tool access** (unauthorized program licence, ECU reprogramming )

**Proximity access** (Wifi/Bluetooth)


**Physical access** (Using OBD connector, tampering with ECU's and/or CAN buses)

**Remote access**

- Telecom network access (radio / base station)
- VPN entry points (Back-office)
- Portals exposed to the Internet

# Attacks on infrastructure

## ElectriCity – Bus 55

- Wireless connection
- Charging stations, 600+ Volts
  - Safety implications
- Supplier / consumer
  - Threat of fraud (billing)

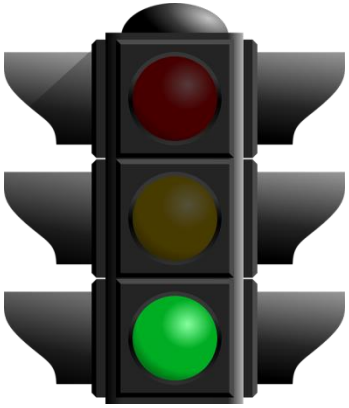

- Something to think about:
  - Impact on society of a cyber attack on the power grid from transportation point of view: Electrical vs fossil fuel vehicles?

# Attacks on infrastructure

## V2I – Example use cases and threats

- **Road works warning**
  - False warnings
  - Jamming legitimate information

- **Green light priority** (heavy vehicles wear down pavement more when stopped. Energy consuming to decelerate and accelerate)
  - Cheating. Attackers getting green light.
  - Traffic disruption by spoofing heavy traffic ( or emergency service vehicles)



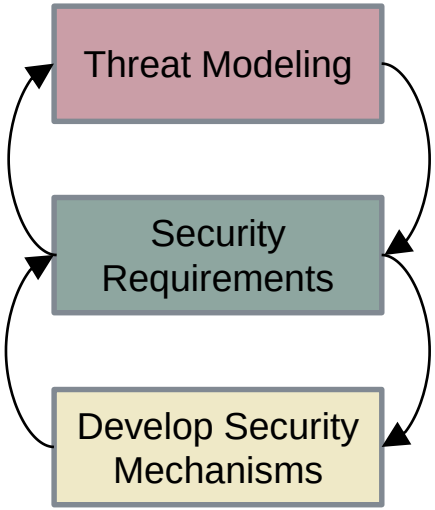
# Security Engineering principle

The principle for Security Engineering is a **risk based approach**.

Security requirements are derived using a

**structured engineering process** and based on:

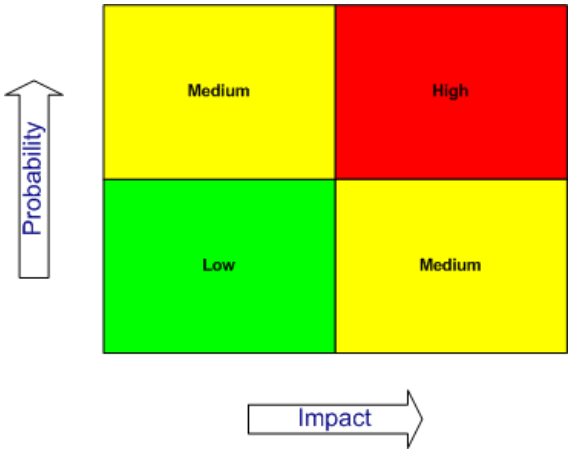
- identification of threats
- risk assessment (likelihood and impact)
- mitigate or accept the risk associated with the threat

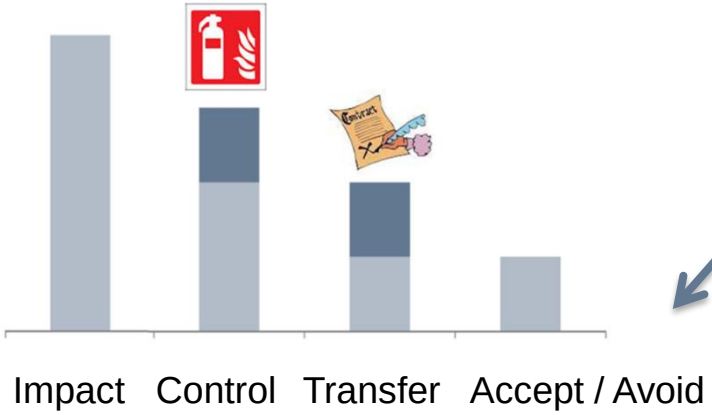



Source: Myagmar, Yurcik

**Note**: Mature areas can have standardized, minimum security requirements (compliance)

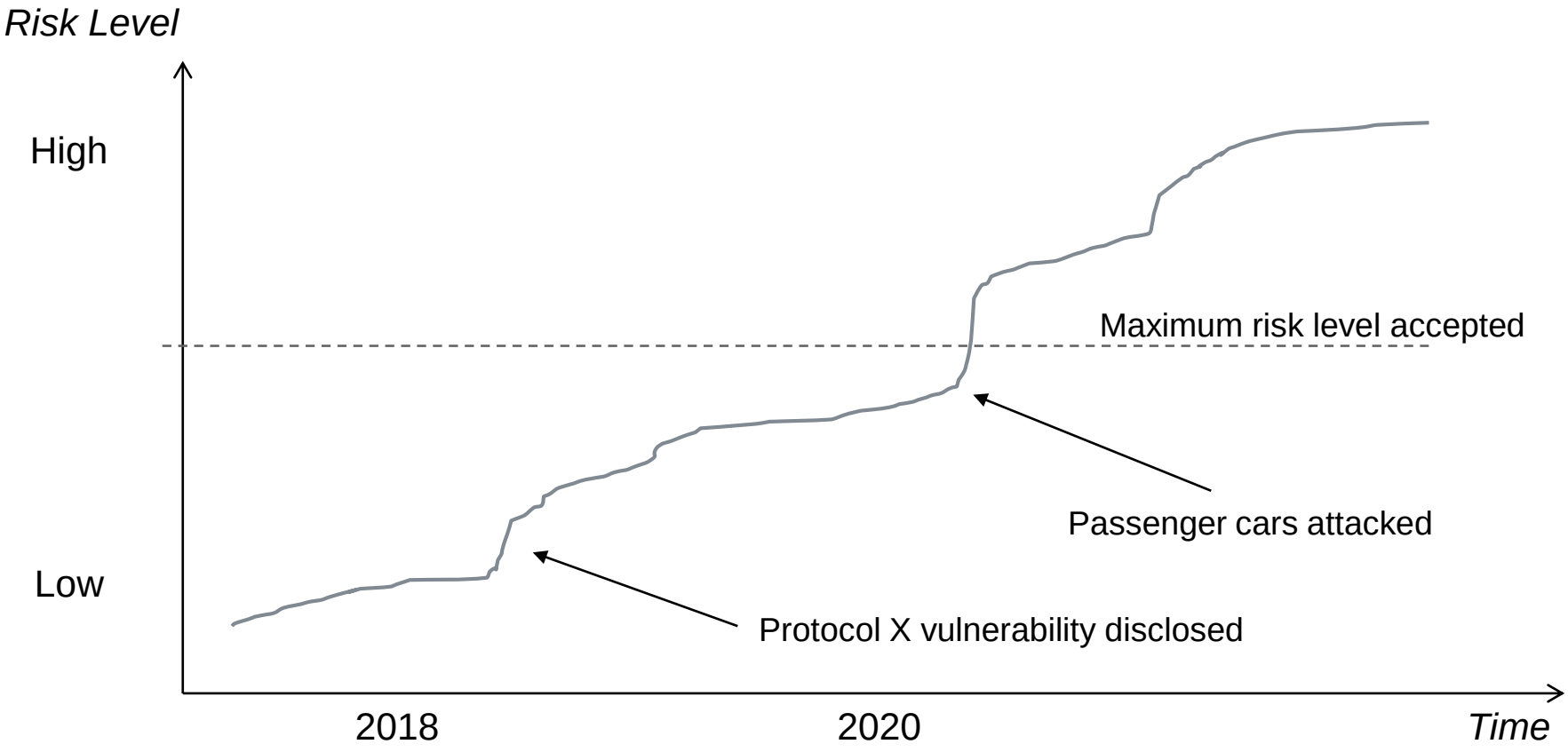
# Risk Management
## - A very quick introduction




Accepted Risk

# Security risks are dynamic
## - risk level at product release will not remain



# Cybersecurity and Vehicle Lifecycle

**Implement Security:**
- Secure Software Design
- Secure Hardware Design
- Perform code review
- Manage third party software

**Maintain Security:**
- Threat Intelligence
- Vulnerability and Patch management
- Incident Response

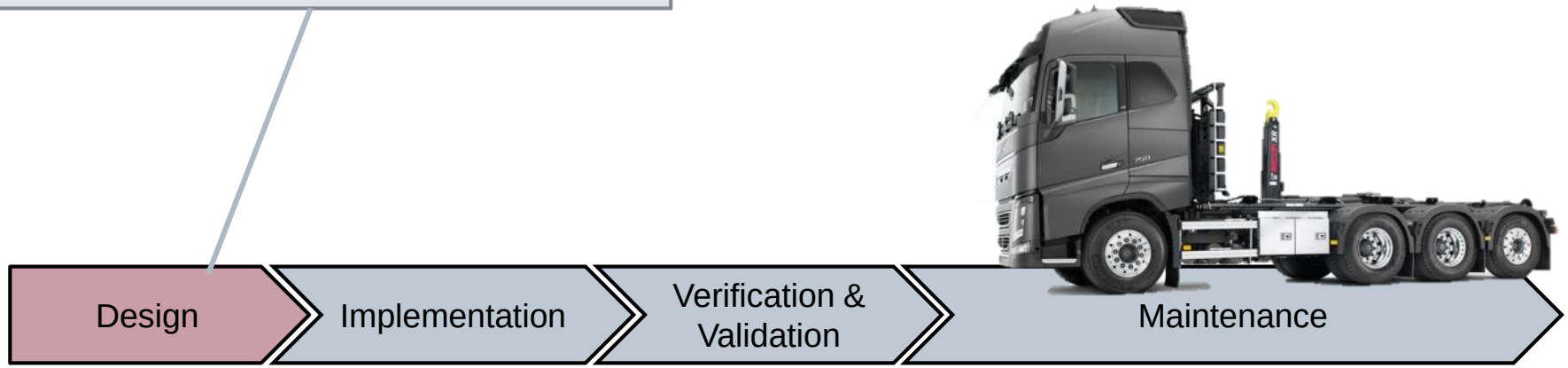
**Design for Security:**
- Formulate Security Objectives
- Perform Threat Analysis and Risk Assessment
- Derive Business Security Requirements
- Develop Security Concept

**Assess Security:**
- Perform Functional Testing
- Perform Vulnerability Testing
- Perform Penetration Testing
- Perform Final Cybersecurity Review

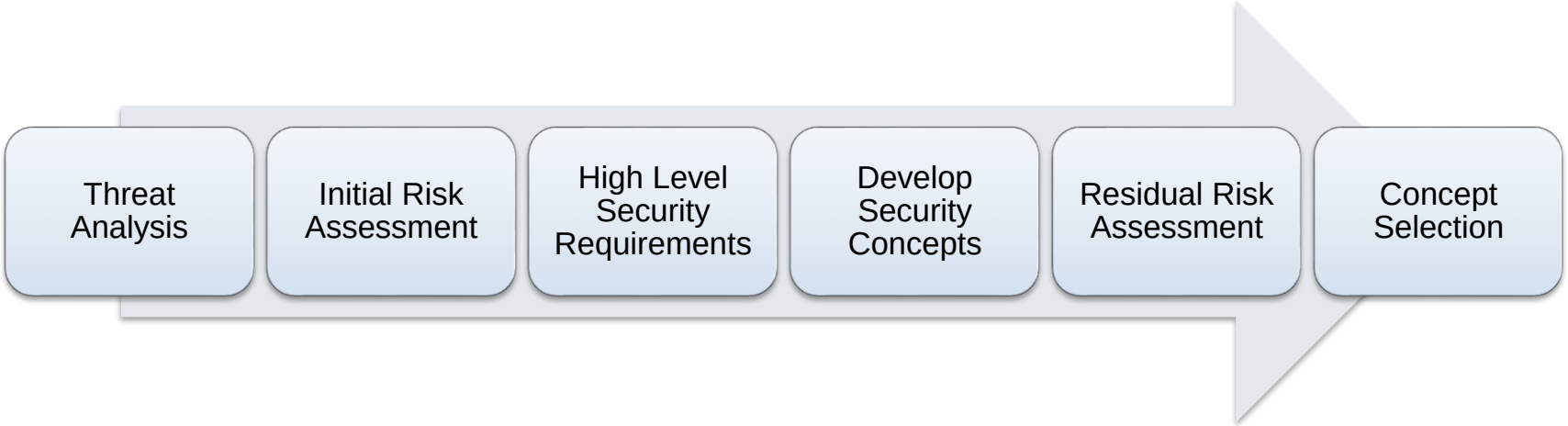
Design → Implementation → Verification & Validation → Maintenance

# Design for Security

**Design for Security:**
- Formulate Security Objectives
- Perform Threat Analysis and Risk Assessment
- Derive Business Security Requirements
- Develop Security Concept



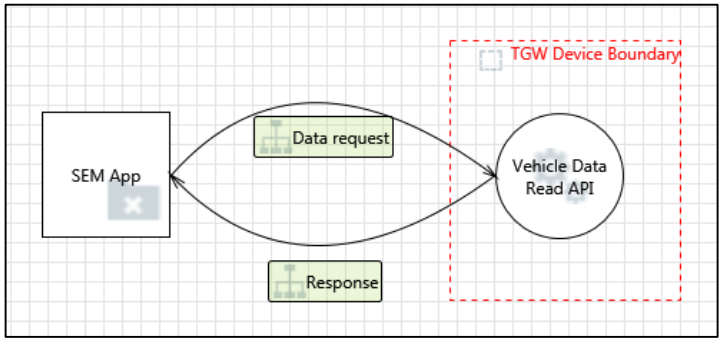
# Design for Security




- Threat Analysis to identify possible cybersecurity threats.
- Assess impact level of the identified threats/attacks (less focus on threat level)
- Formulate high level security requirements to mitigate the identified risks.
- Develop security concepts to be implemented.
- Assess Threat Level considering the security concepts in place
- Results in residual design risks (Accept or Avoid)

# Threat Analysis & Risk assessment

- System model
- STRIDE analysis




| | A | B | C | D |
|---|---|---|---|---|
| 1 | | HEAVENS Risk assessment tool | | |
| 2 | | | | |
| 3 | Id | Asset / Element | Threat | Attack example |
| 4 | 1 | Process X | Spoofing | |
| 5 | 2 | Process X | Tampering | |
| 6 | 3 | Process X | Repudiation | |
| 7 | 4 | Process X | InformationDisclosure | |
| 8 | 5 | Process X | DenialOfService | |
| 9 | 6 | Process X | ElevationOfPrivilege | |
| 10 | 7 | Data Flow Y | Tampering | |
| 11 | 8 | Data Flow Y | InformationDisclosure | |
| 12 | 9 | Data Flow Y | DenialOfService | |
| 13 | 10 | | | |
| 14 | 11 | | | |
| 15 | 12 | | | |

## Threat level

(Expertise, Equipment, Knowledge about TOE, Window of opportunity...)

## Impact level

(Safety, Operational, Privacy/Legislation, Financial)

| Security Level (SL) | | Impact Level (IL) | | | | |
|---|---|---|---|---|---|---|
| | | 0 | 1 | 2 | 3 | 4 |
| Threat Level (TL) | 0 | QM | QM | QM | QM | Low |
| | 1 | QM | Low | Low | Low | Medium |
| | 2 | QM | Low | Medium | Medium | High |
| | 3 | QM | Low | Medium | High | High |
| | 4 | Low | Medium | High | High | Critical |

# Security Requirements

- After determining the risk for identified threats, security requirements can be derived for each threat

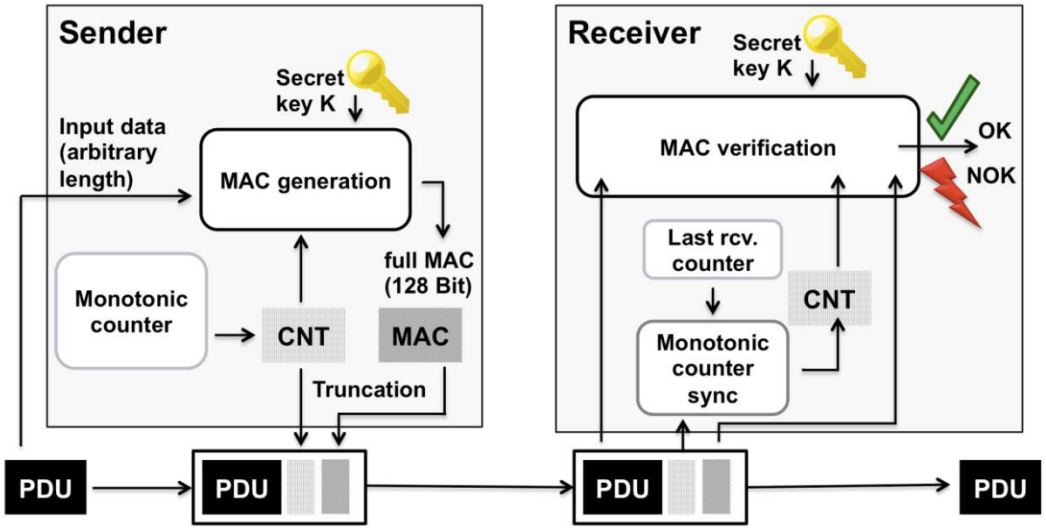
| No. | Asset | Threat | Security Attribute | Security Level |
|---|---|---|---|---|
| 1 | Vehicle Data Response | Tampering of Vehicle Data Response | Integrity | Low |
| … | | | | |

- High level security requirement #1:
  **The integrity of the Vehicle Data Response shall be ensured**

# Example of a Security Concept

**Security Requirement: The integrity of message X shall be ensured**

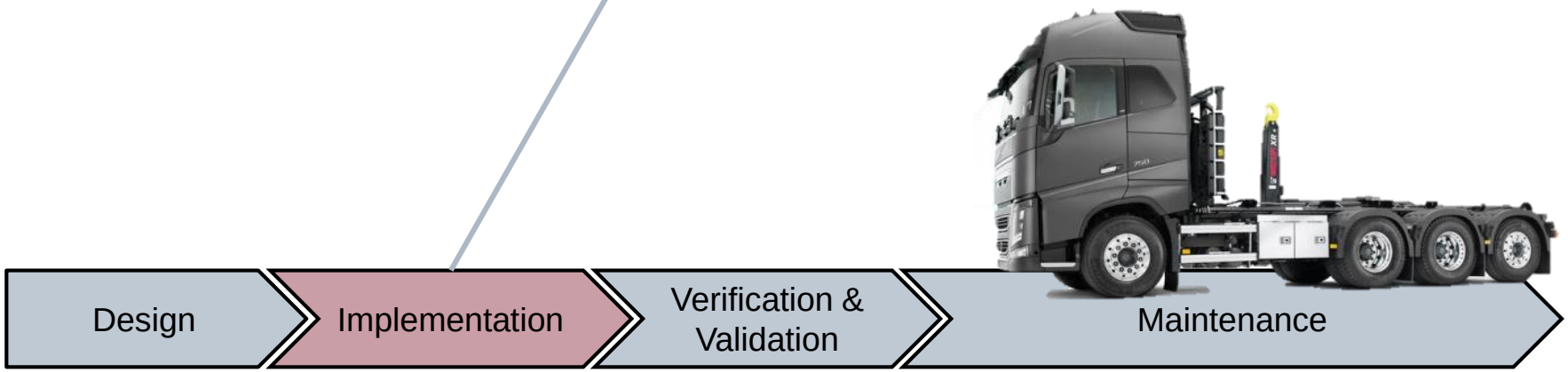
- Integrity protection is e.g. included in AUTOSAR Secure Onboard Communication protocol (adding message authentication codes (MAC) to the original data)




- Mechanism clear, but security relies on good key management

# Implement Security

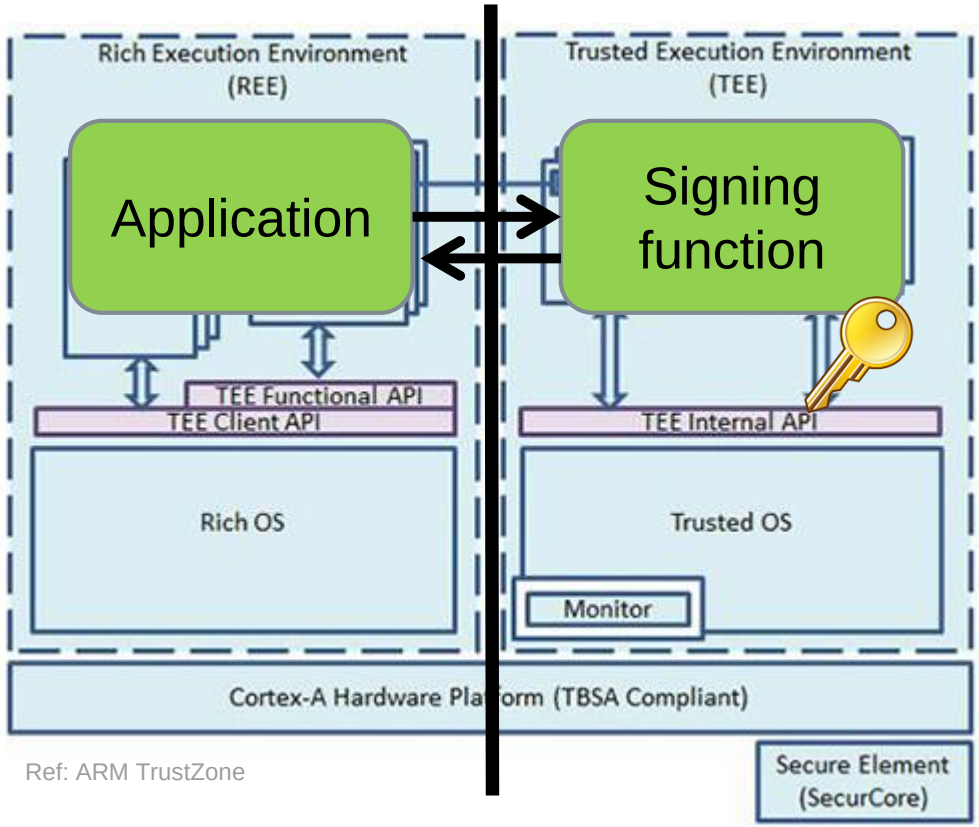
**Implement Security:**
- Secure Software Design
- Secure Hardware Design
- Perform code review
- Manage third party software



# Software composition analysis


Ref: Synopsys Protecode SC

# Software and Hardware design
## - Example of isolated execution environment




Ref: ARM TrustZone

**Example use**

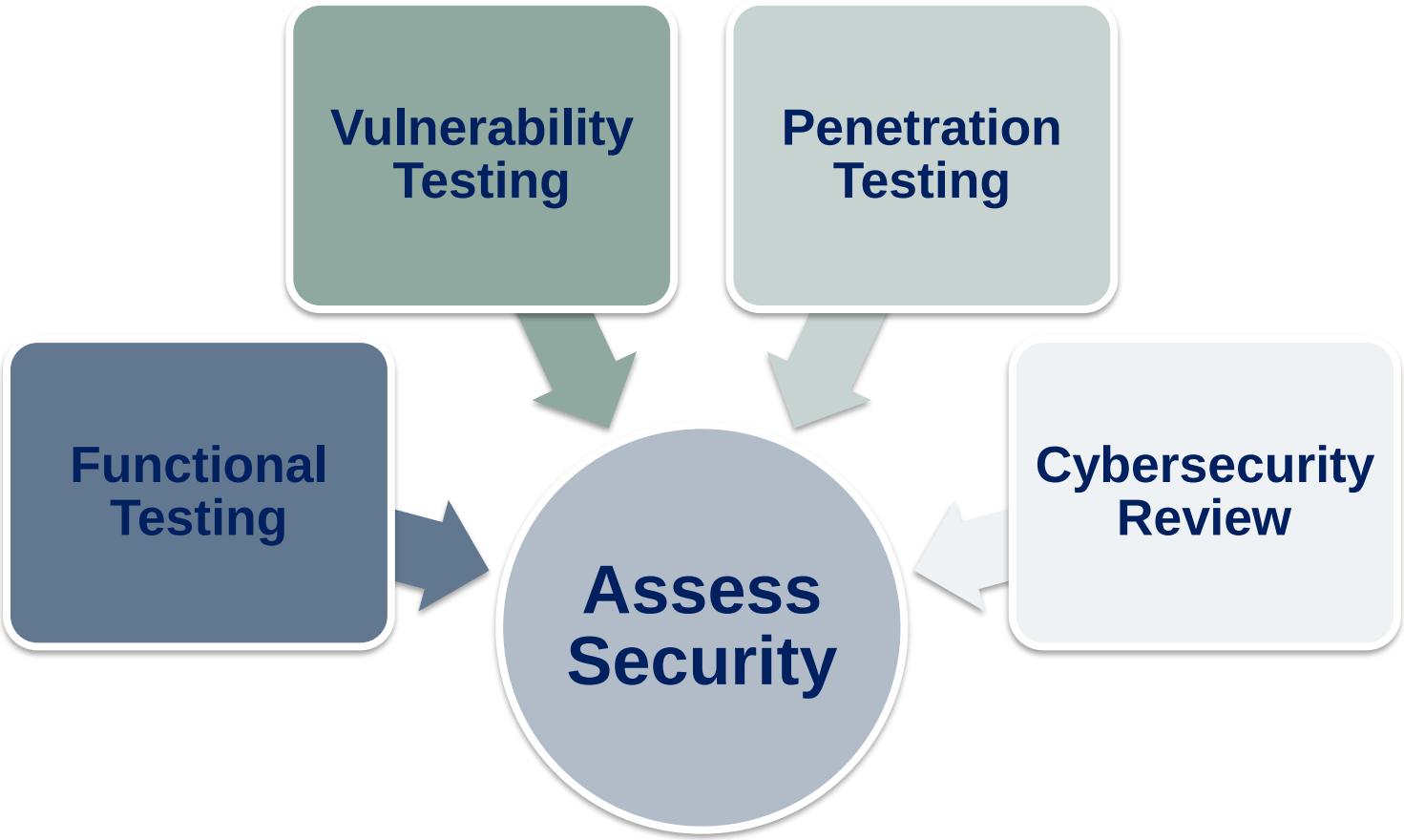
- Need to protect access to private key
- Application can sign data, but have no access to key
- Even if attacker compromise application, private key is not compromised

# Assess Security

**Assess Security:**
- Perform Functional Testing
- Perform Vulnerability Testing
- Perform Penetration Testing
- Perform Final Cybersecurity Review

Design → Implementation → Verification & Validation → Maintenance

# Assess Security

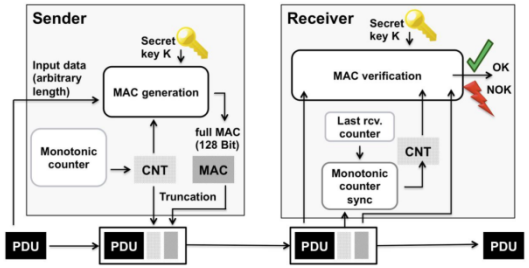


# Functional testing
## - verify correct implementation of security measures

### Correctness
- Positive testing of Algorithms, Protocols, Key Management
- AES, TLS, SecOC, etc

### Robustness
- Negative testing, security measures fail correctly
- Abuse the security measures

### Performance
- Execution time, memory usage



# Vulnerability and Fuzz testing
## - search for known and unknown vulnerabilities

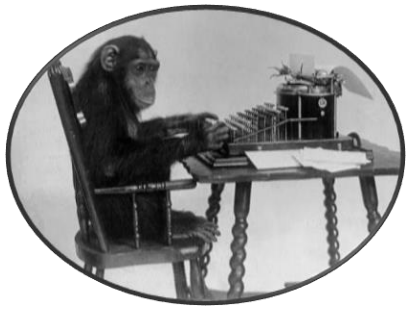
### Known vulnerabilites

- Scan for open ports, services exposed.
- Verify known vulnerabilities patched
- Software Composition analysis

| | Product Name | Vendor Name | Product Type | Number of Vulnerabiliti |
|---|---|---|---|---|
| 1 | Linux Kernel | Linux | OS | 209 |
| 2 | Android | Google | OS | 159 |
| 3 | Imagemagick | Imagemagick | Application | 108 |
| 4 | Iphone Os | Apple | OS | 107 |
| 5 | Mac Os X | Apple | OS | 79 |
| | Windows Server 2008 | Microsoft | OS | |
| | Windows 7 | Microsoft | OS | |
| | Vista | Microsoft | OS | |
| | | Debian | OS | |
| | | Google | Application | |

### Unknown vulnerabilites

- Fuzzing, expose interfaces to unexpected input
- Generation-based, protocol aware
- Robustness



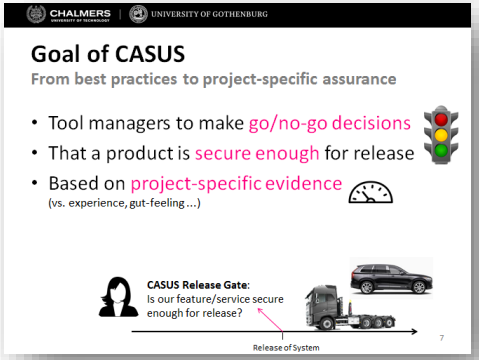
# Final Cybersecurity Review
## - is the system secure enough for release?

Recommended in ISO-SAE 21434 and SAE J3061 (process frameworks)

Review threats, review test results

But how to argue reasonable effort spent to secure vehicle?

PhD position in research project CASUS




Ref: Riccardo Scandariato

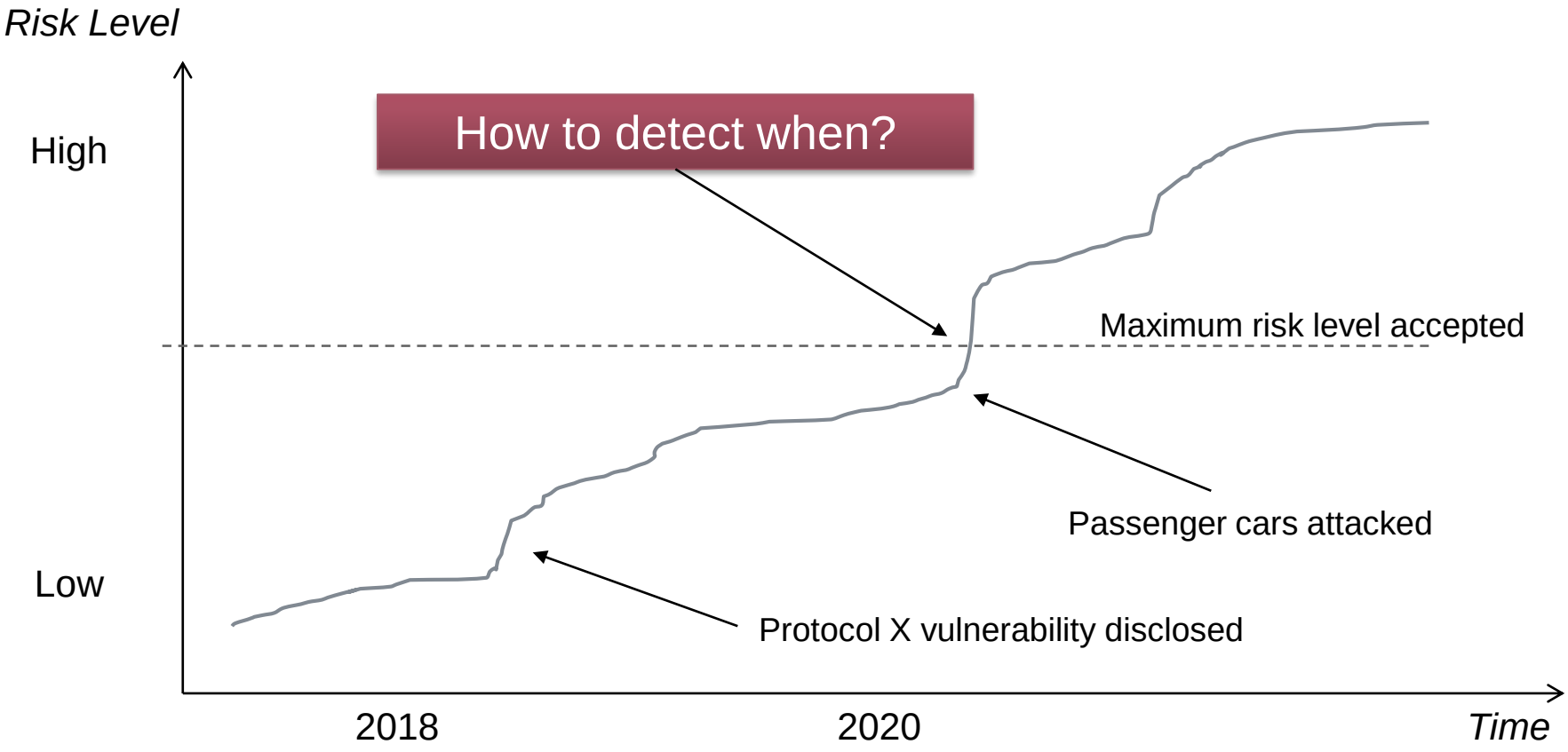
# Maintain Security

**Maintain Security:**
- Threat Intelligence
- Vulnerability and Patch management
- Incident Response

Design → Implementation → Verification & Validation → Maintenance

# Remember?

## - Threat and vulnerabilities change over time



# Vulnerability Management

Mainly related to mitigating from **known software vulnerabilities**.

The process is **proactive**, defend against known vulnerabilities **before attacks** take place.

Common types:

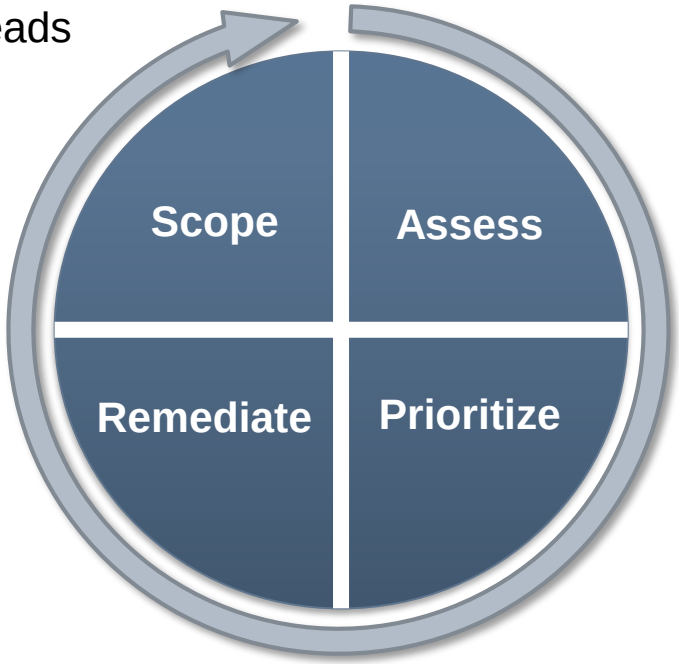
- Buffer overflow, over-reads
- Lack of input validation
- Code injection

esearch for security patches *April 5 2017*

**Top 50 Products By Total Number Of "Distinct" Vulnerabilities in 2017**

Go to year: 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 201
Leaders

| | Product Name | Vendor Name | Product Type | Number of Vulnerabilities |
|---|---|---|---|---|
| 1 | Linux Kernel | Linux | OS | 209 |
| 2 | Android | Google | OS | 159 |
| 3 | Imagemagick | Imagemagick | Application | 108 |
| 4 | Iphone Os | Apple | OS | 107 |
| 5 | Mac Os X | Apple | OS | 79 |
| 6 | Windows Server 2008 | Microsoft | OS | 62 |
| 7 | Windows 7 | Microsoft | OS | 59 |
| 8 | Windows Vista | Microsoft | OS | 58 |
| 9 | Debian Linux | Debian | OS | 57 |
| 10 | Chrome | Google | Application | 5 |




**Scope**

- Asset inventory
- Schedule

**Assess**

- Vulnerabilities feeds
- Scan / research assets
- Determine relevance

**Prioritize**

- Assess risk
- Plan actions

**Remediate**

- Deploy security updates
- Report progress

# The bigger picture
## - Holistic Cybersecurity Management

# Opportunities for students

**Summer job** **Thesis work** **Internship**

https://www.volvogroup.com/en-en/careers/opportunities-for-students.html

# Questions