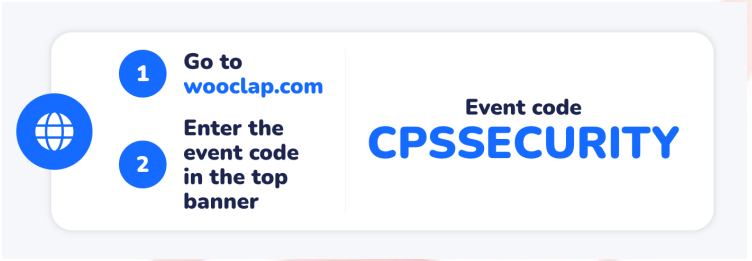
CE/CZ4055 Cyber Physical System Security

Automotive Cyber Security

Anupam Chattopadhyay

SCSE, NTU



NANYANG TECHNOLOGICAL UNIVERSITY

Quiz 2 Solutions

1. **Multiple Choice: 1: Following is _not_ a property of Phys...**

Question	Following is _not_ a property of Physically Unclonable Function (PUF)
Answer	✓ Fast
	Unique
	Unclonable
	Evaluatable

2. **Multiple Choice: 2: Meltdown attack exploits**

Question	Meltdown attack exploits
Answer	✓ Speculative execution of tasks
	Correct execution of tasks
	Incorrect execution of tasks
	Deterministic execution of tasks

3. **Multiple Choice: 3: Micro-architectural attack types are**

Question	Micro-architectural attack types are
Answer	✓ Active and Passive
	Sleepy and Awake
	Stochastic and Deterministic
	Fast and Slow

4. **Multiple Choice: 4: Public Key Infrastructure (PKI) addre...**

Question	Public Key Infrastructure (PKI) addresses the following problem
Answer	✓ Key distribution
	Reliability
	Digital Signature
	Access Control

Quiz 2 Solutions

5. **Multiple Choice: 5: For an n-user wireless sensor network...**

Question	For an n-user wireless sensor network, total number of key exchanges can be at most
Answer	✓ n(n-1)/2
	n*n
	n/2
	n!

6. **Multiple Choice: 6: Pairwise key distribution has the fol...**

Question	Pairwise key distribution has the following problem
Answer	✓ High memory requirement
	Too many users
	Weak authenticity
	Security is low

7. **Multiple Choice: 7: Following is not a function of Hardwa...**

Question	Following is *not* a function of Hardware Security Module
Answer	✓ Storing power traces
	Storing private keys
	Generate key pairs
	Provide an audit trail

8. **Multiple Choice: 8: Bluetooth provides security through**

Question	Bluetooth provides security through
Answer	✓ Pairing procedure
	Public key cryptography
	Frequency hopping
	Fast data transfer

Quiz 2 Solutions

9. **Multiple Choice: 9: Following is not an attack on Bluetoo...**

Question	Following is *not* an attack on Bluetooth device
Answer	✓ Decryption attack
	Location privacy attack
	Replay attack
	Device impersonation attack

10. **Multiple Choice: 10: One-way diodes are typically used in**

Question	One-way diodes are typically used in
Answer	✓ SCADA network
	Bluetooth network
	WiFi network
	Wired network

NANYANG TECHNOLOGICAL UNIVERSITY

The BIG Picture

SECURE TRANSPORT

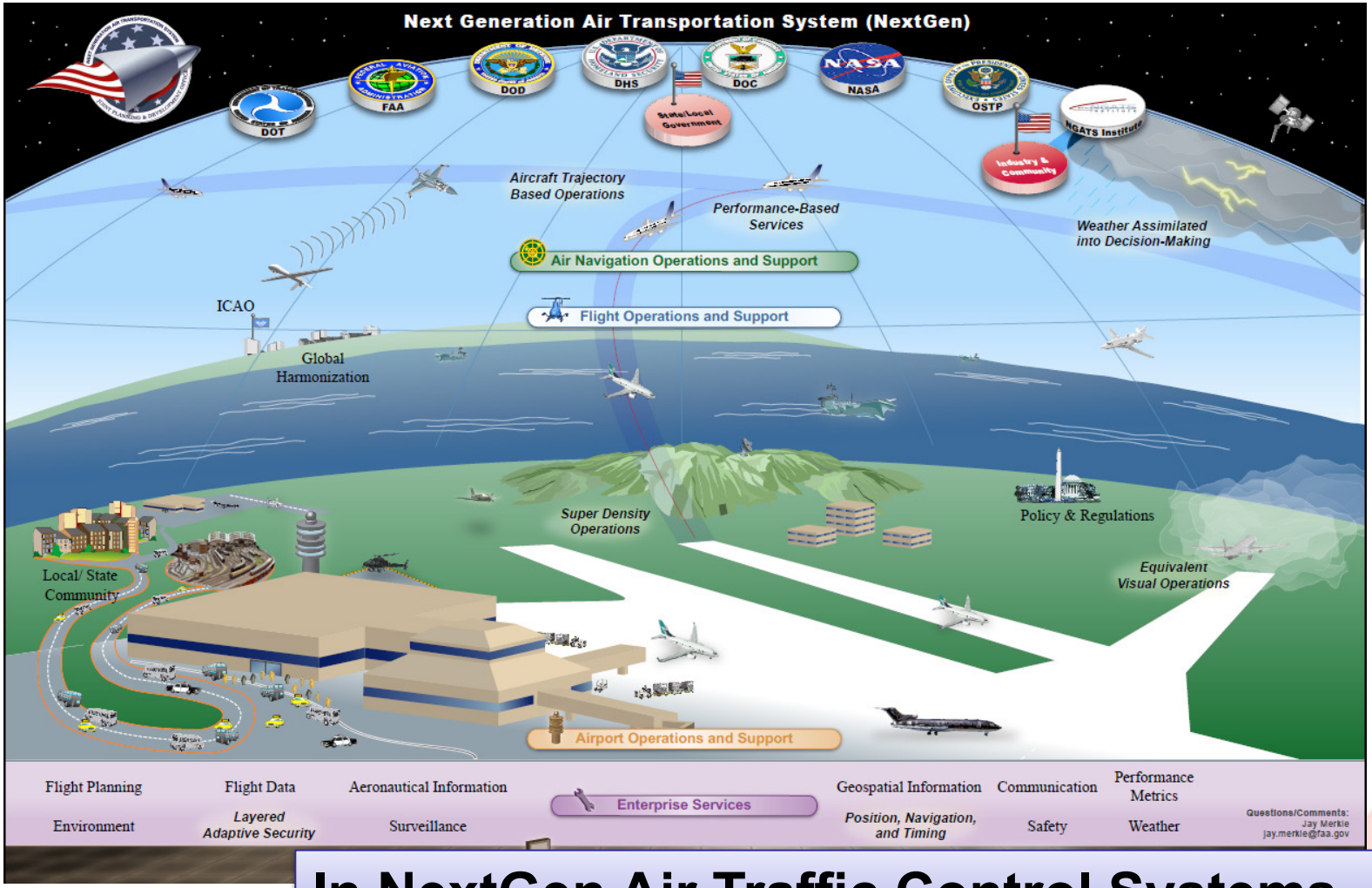
NANYANG TECHNOLOGICAL UNIVERSITY

Intelligent Transportation Systems

Aug 13, 2022: **The auto industry lost its spectrum fight with the Federal Communications Commission.** Europe and many other areas still have a wider spectrum of the 5.9GHz band reserved for V2V and V2X technologies, worldwide harmonisation on the issue is clearly vital in making a truly cohesive intelligent transport system

NANYANG TECHNOLOGICAL UNIVERSITY

Dependence on the Digital Infrastructure



In NextGen Air Traffic Control Systems

NANYANG TECHNOLOGICAL UNIVERSITY

Intermodal Ports

Terminal Operations & Management

Automated Gates

Physical Security

Crane Monitoring and Control

Wireless Devices & Tracking

NANYANG TECHNOLOGICAL UNIVERSITY

Transit Vehicles are E-enabled and Autonomous

RF Cellular WiFi WiMAX DSRC

Control Domain

Vehicle Controls

Vehicle Diagnostics

Traffic Signal Priority

Video Surveillance

Vehicle Immobilizers

Operations Domain

Automated Dispatching

Vehicle Location

Route/Schedule Status

Passenger Counters

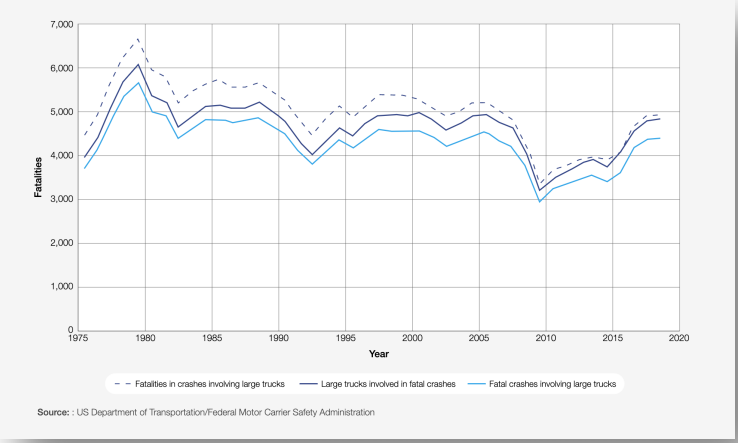
Electronic Payments

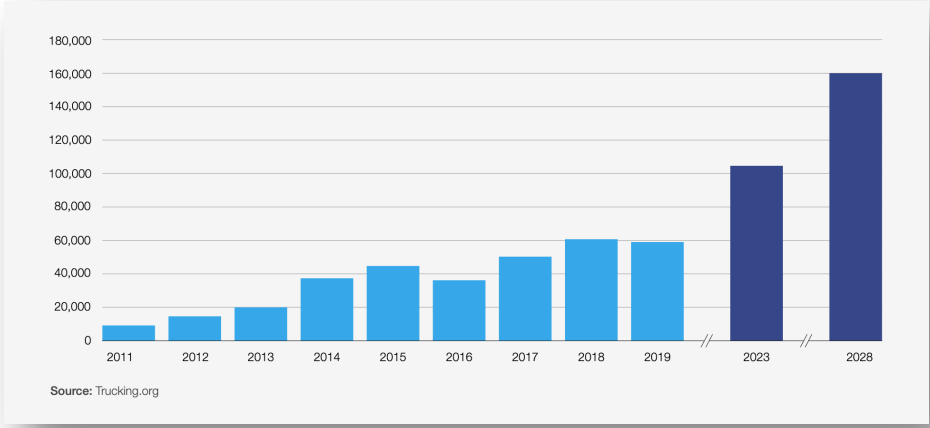
Infotainment Domain

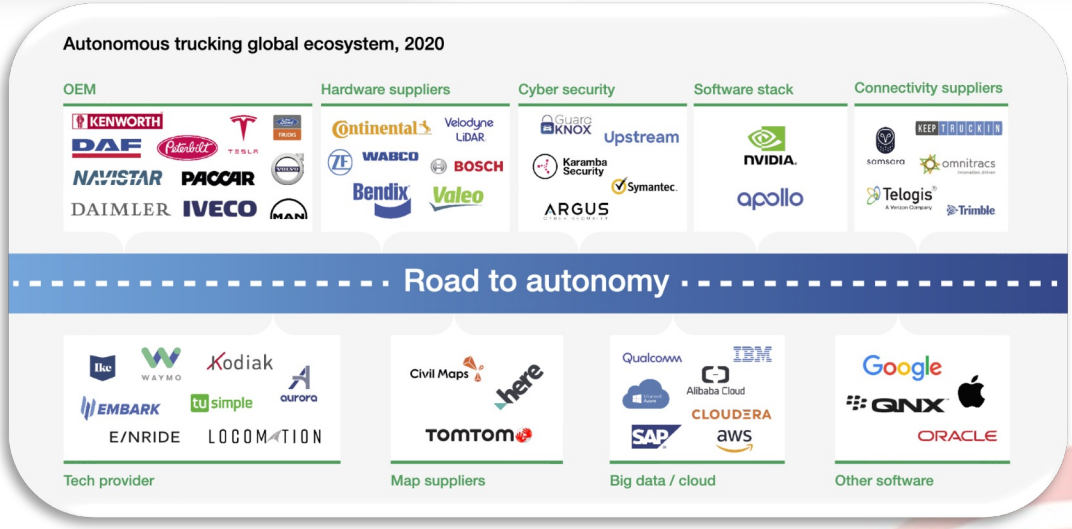
Customer use of WiFi and WiMAX **Real-time Travel Info, Trip Planning**

NANYANG TECHNOLOGICAL UNIVERSITY

Autonomy addresses Fatalities, Driver Shortage

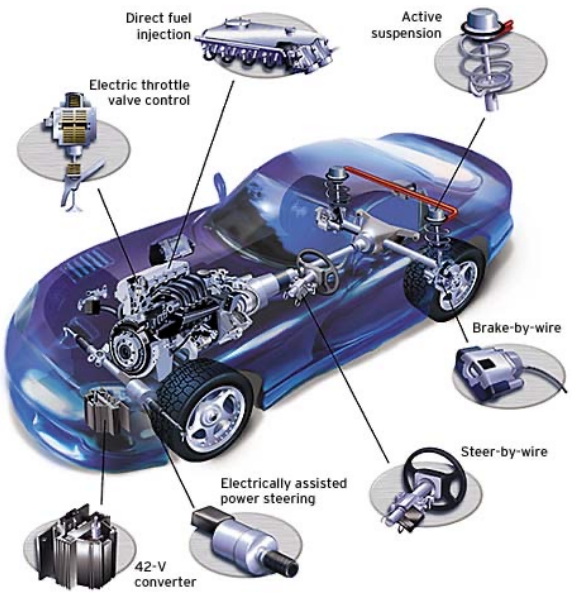


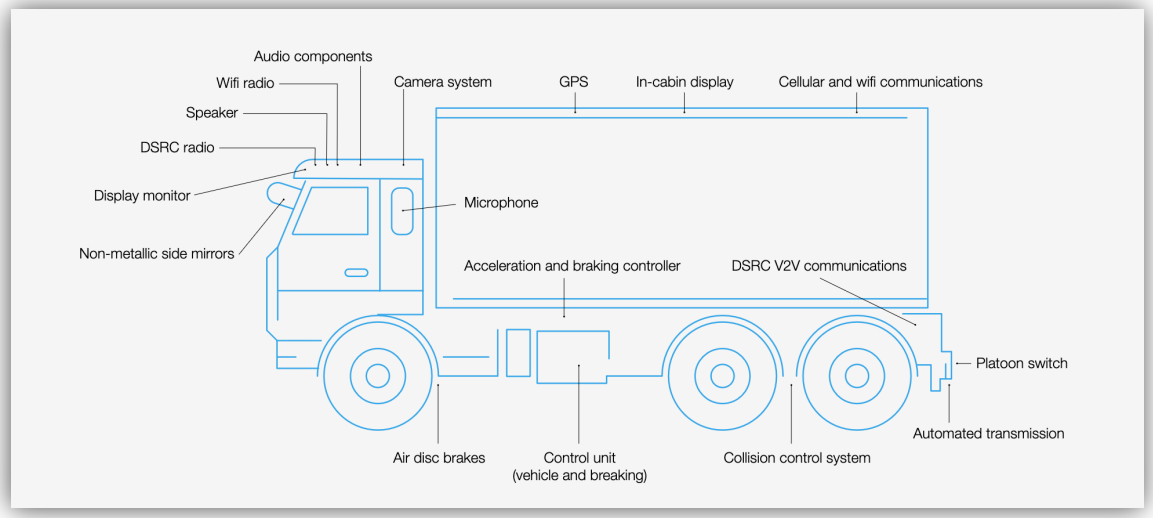




NANYANG TECHNOLOGICAL UNIVERSITY

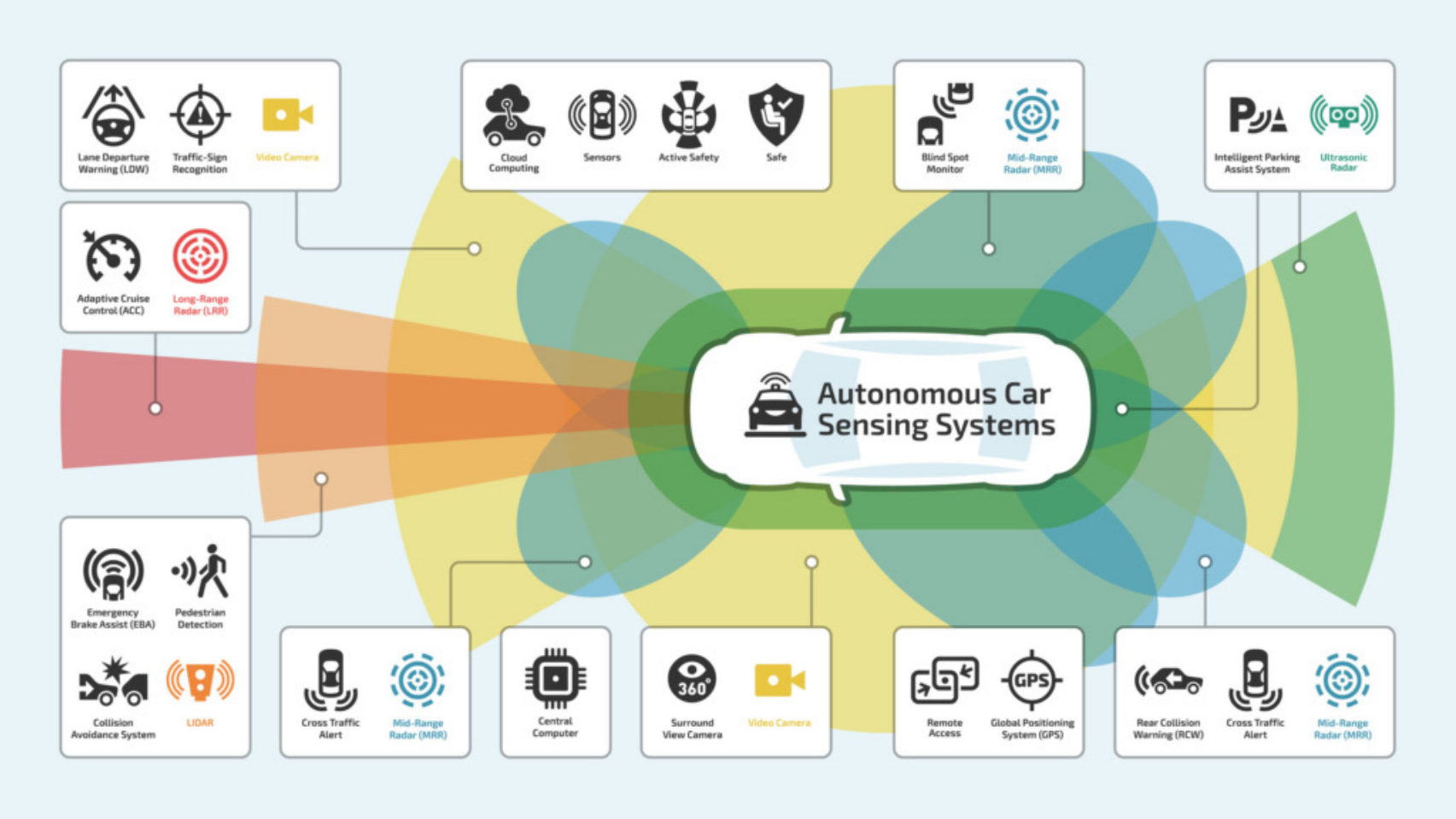
Automobiles and Trucks Are E-enabled





NANYANG TECHNOLOGICAL UNIVERSITY

Powered by Sensors



NANYANG TECHNOLOGICAL UNIVERSITY

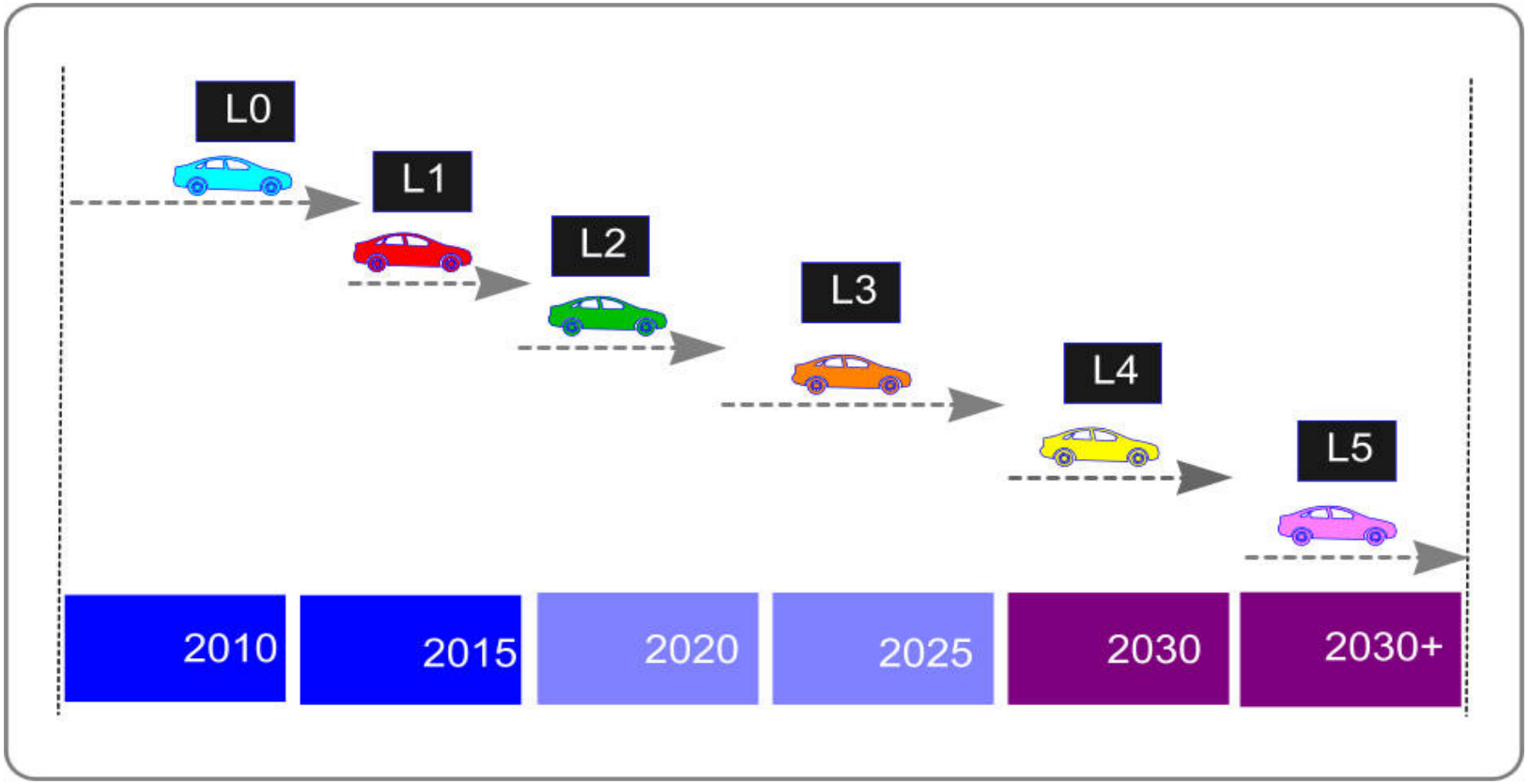
Increasing Autonomy

Level	Automation	Steering Cruise	Environment Monitoring	Fallback Control	Driving Modes
0	None	H	H	H	N/A
1	Supportive	H,S	H	H	Some
2	Partial	S	H	H	Some
3	Conditional	S	S	H	Some
4	High	S	S	H	Some
5	Full	S	S	S	All

TABLE I
AUTONOMOUS VEHICLES: LEVELS OF AUTONOMY (*S* - SYSTEM, *H* - HUMAN)

Society of Automotive Engineers: *standard* ***SAE J3016*** *defines classes of vehicle automation*

Technology Timeline



Multiple generations of technology will co-exist on our roads for many years.

Recent Highlights

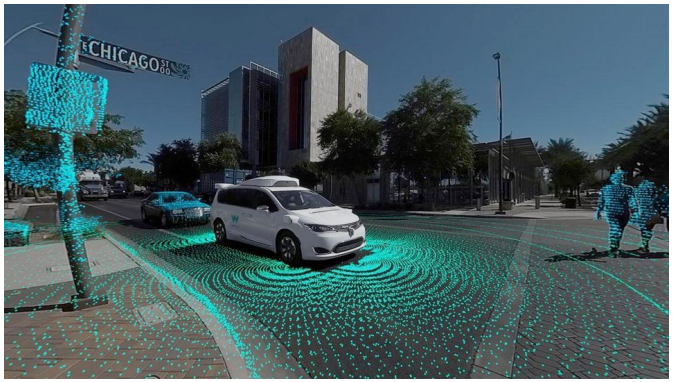


Photo Courtesy: Waymo

- **SAE J3016** has been formally validated by the US Department of Transport
- **Tesla Motors Inc**., BMW, Ford Motor Co. and Volvo Cars have all promised to have fully autonomous cars on the road within five years
- **Alphabet Inc.'s** (Google) autonomous test vehicles, Waymo, has amassed 7+ Million miles by December, 2023
  - 0.41 incidents per million miles (compared to 2.78 incident per million miles for human)
- **China** has set a goal for 10-20% of vehicles to be highly autonomous by 2025, and for 10% of cars to be fully self-driving in 2030
- **Nvidia** and Mercedes-Benz announced intention to develop "cognitive car" using embedded AI technology

Cyber Security is One of the Most Serious Potential Risks in Transportation

- Increasing dependence on information systems and networks
- Risks are significant and growing
- Need a comprehensive approach
- Need a culture/ecosystem of cyber security
- Cyber security is necessary for transportation mobility and safety!

NANYANG TECHNOLOGICAL UNIVERSITY

Insider Threat Impacted Traffic Management Center and Signaling

- *Ghena et al, "Green Lights Forever: Analyzing the Security of Traffic Infrastructure", USENIX 2014*
- *A. Greenberg, "Why the Belarus Railways Hack Marks a First for Ransomware", Wired, January, 2022*

NANYANG TECHNOLOGICAL UNIVERSITY

- ”Tesla Model 3 Hacked in Less Than 2 Minutes at **Pwn2Own Contest**”, March, 2023
  - Attack I: Hacked Tesla’s Gateway Energy Management System in *less than 2 minutes*
  - Attack II: Exploited a *heap overflow vulnerability* and an *out-of-bounds write error* in a *Bluetooth chipset* to break into Tesla's infotainment system and, from there, gain root access to other subsystems

Contents

- *Automotive Security Incidents*
- Attack Models and Standardization
- Security by Design
- Discussion

NANYANG TECHNOLOGICAL UNIVERSITY

Threat Model

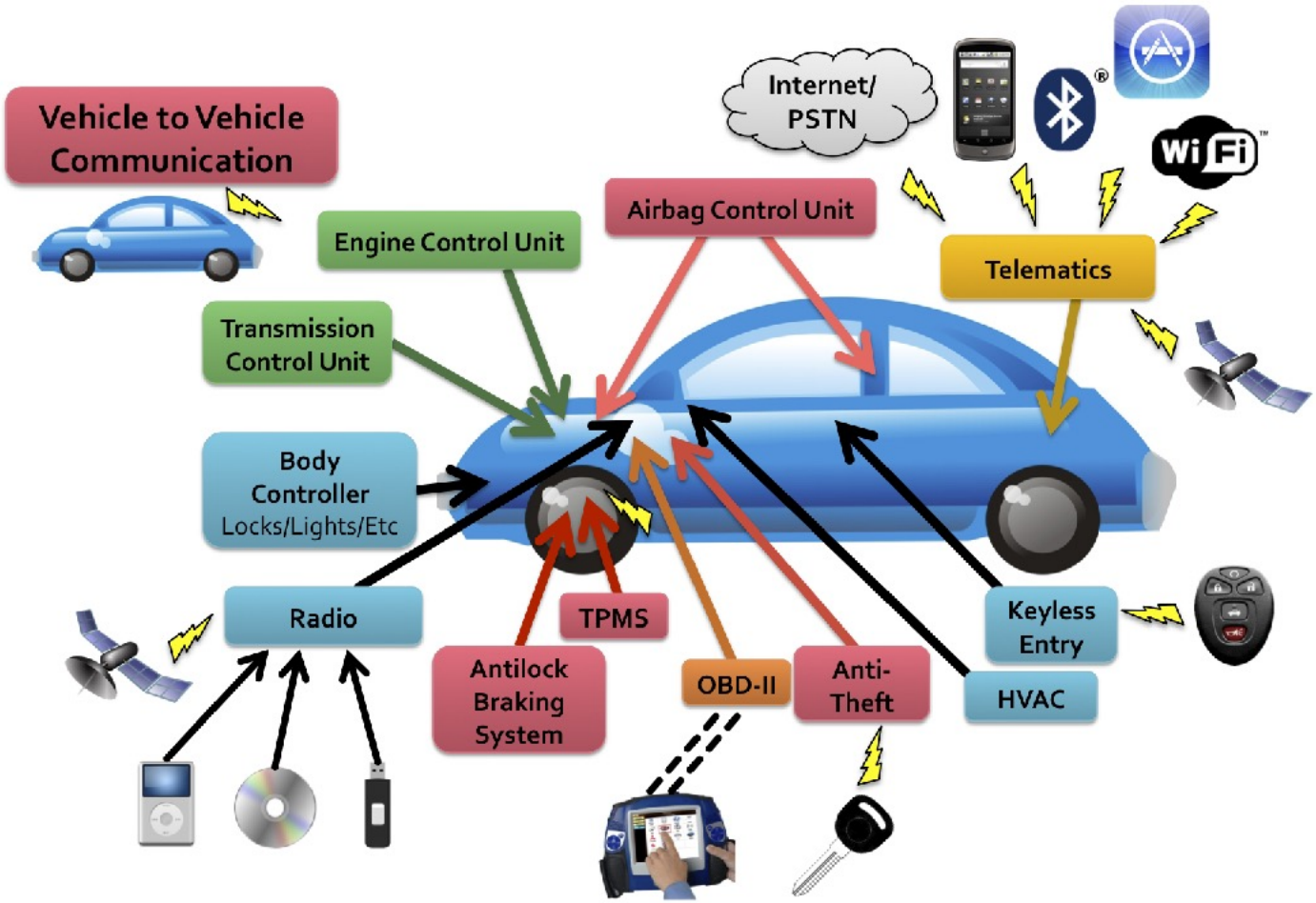
- Technical Capabilities
  - Capabilities in analyzing the system and developing exploits
- Operational capabilities
  - Analysis of attack surface of vehicles
  - How malicious payload is delivered
  - Indirect physical access, short-range wireless, long-range wireless accesses

Chekoway et al, "Comprehensive Experimental Analyses of Automotive Attack Surfaces", USENIX 2011

Vehicle attack surface

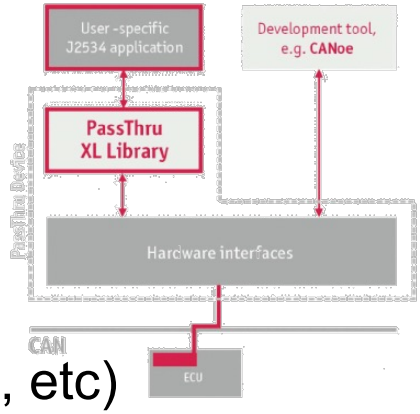
- Short-range wireless access
  - Bluetooth, Remote Keyless Entry, Tire Pressure (TPMS), WiFi
- Long-range wireless access
  - GPS, Satellite radio, Digital radio
- OBD-II
  - On board diagnostics II
  - Connects to all key CAN buses of vehicle
  - Used during vehicle maintenance
- Entertainment : Disc, USB, iPod

Vehicle attack surface



Vulnerability Analysis

- Focused on moderately priced sedan with standard options and components
- Cars < 30 ECUS comprising both critical drivetrain components & less critical components
- **PassThru** for ECU diagnosis and reprogramming



Every vulnerability allowed complete control

- General Procedure:
  - Identify microprocessor (PowerPC, ARM, Super-H, etc)
  - Extract firmware and reverse engineer using debugging devices/software where possible
  - Exploit vulnerability or simply reprogram ECU

Chekoway et al, "Comprehensive Experimental Analyses of Automotive Attack Surfaces", USENIX 2011

Exploitation Summary

Vulnerability Class	Channel	Implemented Capability	Visible to User	Scale	Full Control	Cost	Section
Direct physical	OBD-II port	Plug attack hardware directly into car OBD-II port	Yes	Small	Yes	Low	Prior work [14]
Indirect physical	CD	CD-based firmware update	Yes	Small	Yes	Medium	Section 4.2
	CD	Special song (WMA)	Yes*	Medium	Yes	Medium-High	Section 4.2
	PassThru	WiFi or wired control connection to advertised PassThru devices	No	Small	Yes	Low	Section 4.2
	PassThru	WiFi or wired shell injection	No	Viral	Yes	Low	Section 4.2
Short-range wireless	Bluetooth	Buffer overflow with paired Android phone and Trojan app	No	Large	Yes	Low-Medium	Section 4.3
	Bluetooth	Sniff MAC address, brute force PIN, buffer overflow	No	Small	Yes	Low-Medium	Section 4.3
Long-range wireless	Cellular	Call car, authentication exploit, buffer overflow (using laptop)	No	Large	Yes	Medium-High	Section 4.4
	Cellular	Call car, authentication exploit, buffer overflow (using iPod with exploit audio file, earphones, and a telephone)	No	Large	Yes	Medium-High	Section 4.4

Chekoway et al, "Comprehensive Experimental Analyses of Automotive Attack Surfaces", USENIX 2011

Indirect Physical Exploits

Media Player

- Accepts compact discs
- Software running on CPU handles audio parsing, UI functions, handles connections
- Two exploits
  1. Latent update capability of player manufacturer
     - Updates when user does nothing
  2. WMA parser vulnerability
     - Audio file parse correctly on a PC - In vehicle send arbitrary CAN packets

Indirect Physical Exploits

OBD-II

- Looked at PassThru device from manufacturer
- Found no authentication for PC's on same WiFi network
- Found exploit allowing reprogramming of PassThru
  - Allows for PassThru worm
  - Allows for control of vehicle reprogramming
  - Includes unsecured and unused Linux programs

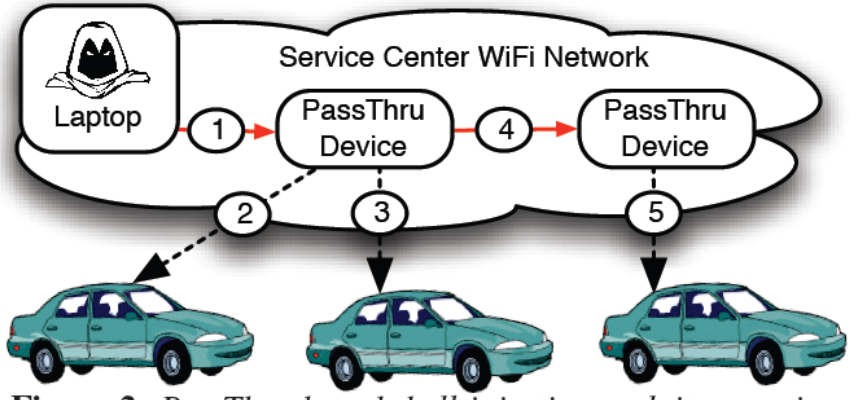


Figure 2: *PassThru-based shell-injection exploit scenario.* The adversary gains access to the service center network (e.g., by compromising an employee laptop), then (1) compromises any PassThru devices on the network, each of which compromise any cars they are used to service (2 and 3), installing Trojan horses to be activated based on some environmental trigger. The PassThru device also (4) spreads virally to other PassThru devices (e.g., if a device is loaned to other shops) which can repeat the same process (5).

NANYANG TECHNOLOGICAL UNIVERSITY

Short-range Wireless Exploitation

Bluetooth

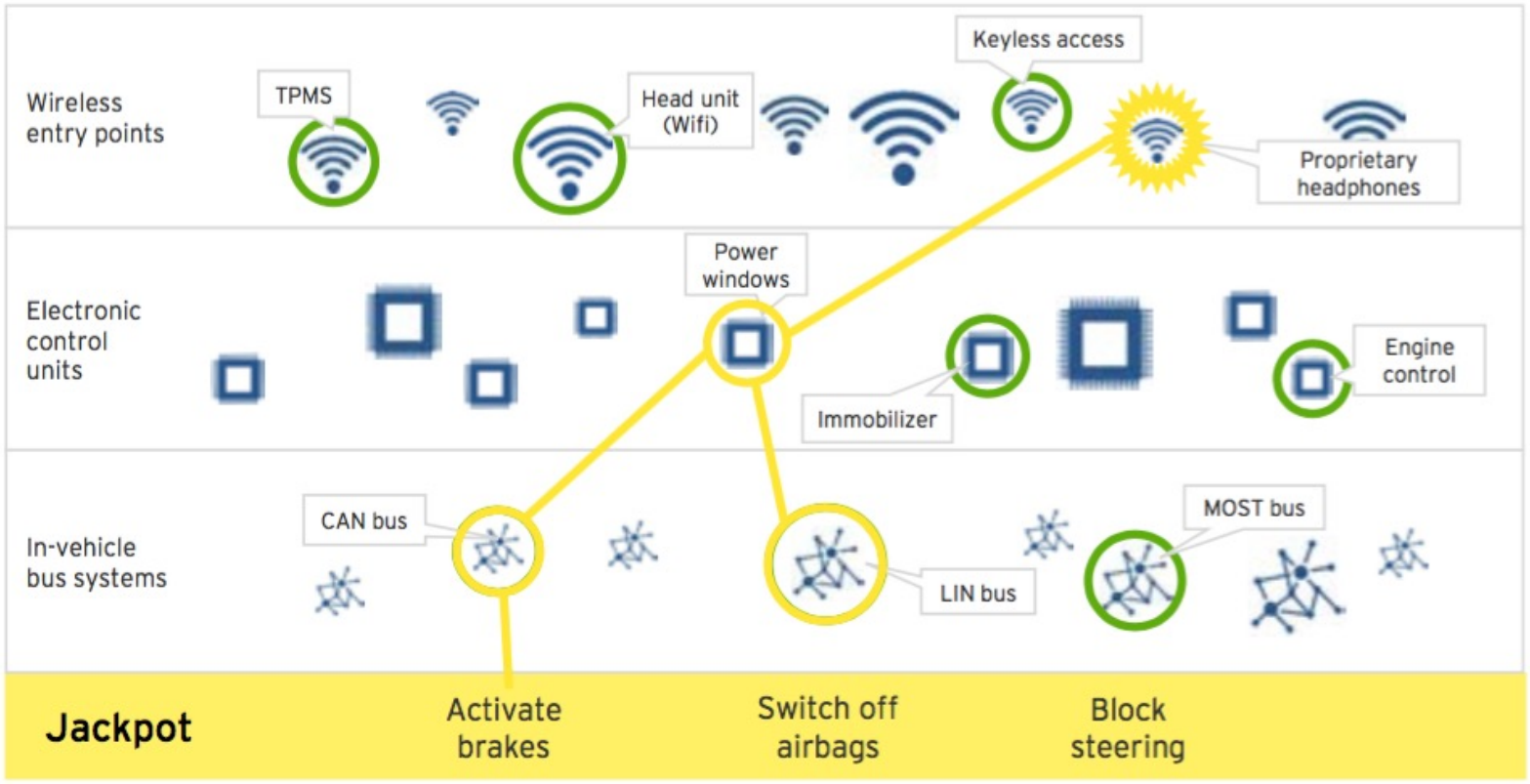
- Found popular Bluetooth protocol stack with custom manufacture code on top
  - Custom code contained 20 unsafe calls to *strcpy()*
- Indirect attack → assumes attacker has paired device
  - Implemented Trojan on Android device to compromise machine
- Direct attack → exploits with a paired device
  - Requires brute force of PIN to pair device (10 hours) → Limited by response of vehicle's Bluetooth

Contents

- Automotive Security Incidents
- *Attack Models and Standardization*
- Security by Design
- Discussion

NANYANG TECHNOLOGICAL UNIVERSITY

Simple Attack Flow



TPMS: Tire Pressure Measurement System
CAN: Controller Area Network
LIN: Local Interconnect Network
MOST: Media Oriented Systems Transport

Automotive Cybersecurity: Problem Description

Threat motivations: Example

Theft

- Stealing sensitive information (e.g., Credit Card details)
- Deploying Ransomware
- Automotive Botnet Attack
  - Able to have cars report Vehicle Identification Number (VIN) and GPS
  - Can unlock doors, start engine and fully startup car
  - Cannot disable steering column lock

Surveillance

- Allows audio recording from in-cabin microphone
- Monitoring locations

Vulnerability: It's Complicated

- Example: the new Ford F150 pickup has 150 million lines of code
- Each vehicle has multiple Electronic Control Units (ECUs) from different vendors
- Presents multiple attack points for hackers
- Complexity is the enemy of security

7 million lines of code

Examples of Risks

Unauthorised access to vehicles	Keyless door entry systems use mobile apps or electronic key-fobs
Theft of personal information	Owner details, GPS logs, Credit Card info, etc.
'Hijacking' of individual vehicles	Feasibility demonstrated by 'Jeep hack' (2015)
Creation of mobile 'bots'	Vehicle software compromised by hackers and used to launch cyber-attacks
Installation of 'ransomware'	Victims must pay money to regain control of their vehicles

Automotive Cybersecurity: Emerging Solutions

SAE J3061

- **"Cybersecurity Guidebook for Cyber-Physical Vehicle Systems" – published January 2016**
- Provides a framework to help organizations
  1. Identify and assess cybersecurity threats related to vehicles
  2. Design cybersecurity into cyber-physical vehicle systems throughout the entire development lifecycle process.
  3. Provides the foundation for further standards development.

OTA Updates

- “Over-the-air” software updates are crucial part of strategy
- Already implemented by vendors such as Tesla Motors
- Needs to be carefully implemented else OTA service can be hacked

Sharing of Expertise

- Automotive Information Sharing Advisory Centre (Auto-ISAC)
  - Established by the Auto industry to facilitate development of cybersecurity expertise within Automotive supply chain
  - “An industry-operated environment created to enhance cyber security awareness and coordination across the global automotive industry”
  - Published set of ‘Best Practices’ for automotive cybersecurity in July 2016

https://www.automotiveisac.com/best-practices/

Improve Software Quality

- Difficult to accurately estimate extent to which software code may deemed 'buggy'
- Major initiatives designed to improve software quality
  - NIST 8151 '*Dramatically Reducing Software Vulnerabilities*'

September 2016: *General Motors announced recall of 3.6 million vehicles after fear that air-bags may fail to deploy due to software fault.*

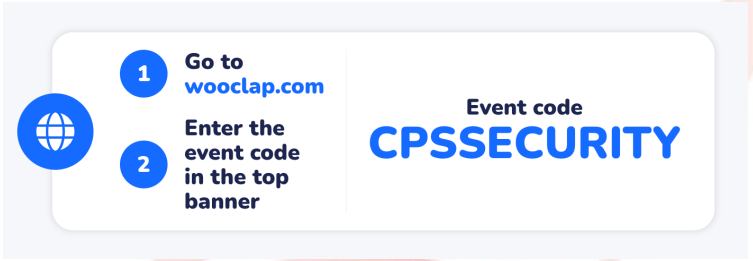
NIST 8151 http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8151.pdf

Security fixes

- Standard security engineering best-practices e.g. don't use unsafe *strcpy* → instead *strncpy*
- Removing debugging and error symbols
- Use stack cookies and Address Space Layout Randomization (ASLR)
- Remove unused services e.g. telnet and ftp
- Authentication before re-flashing

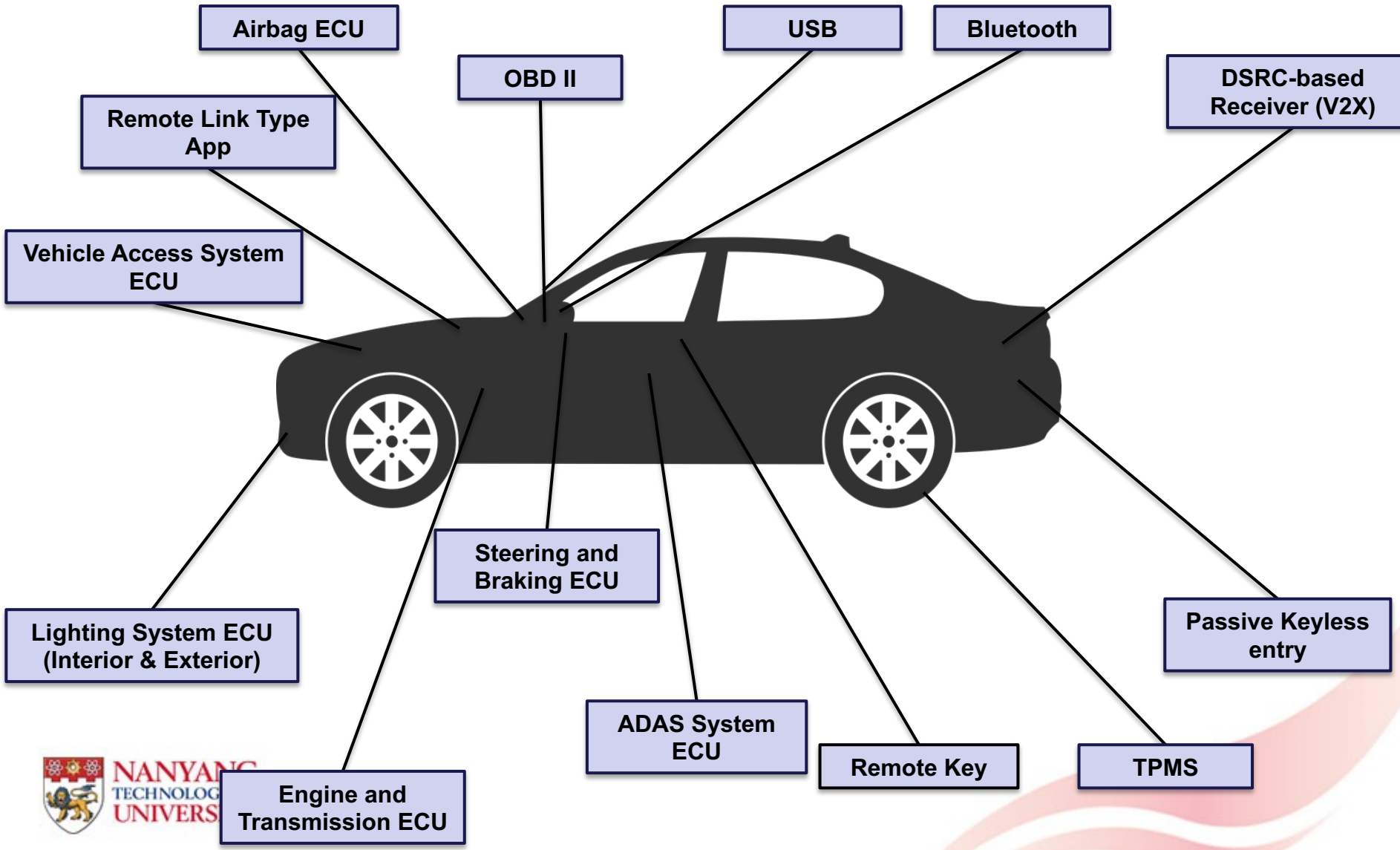
Contents

- Automotive Security Incidents
- Attack Models and Standardization
- *Security by Design*
- Discussion

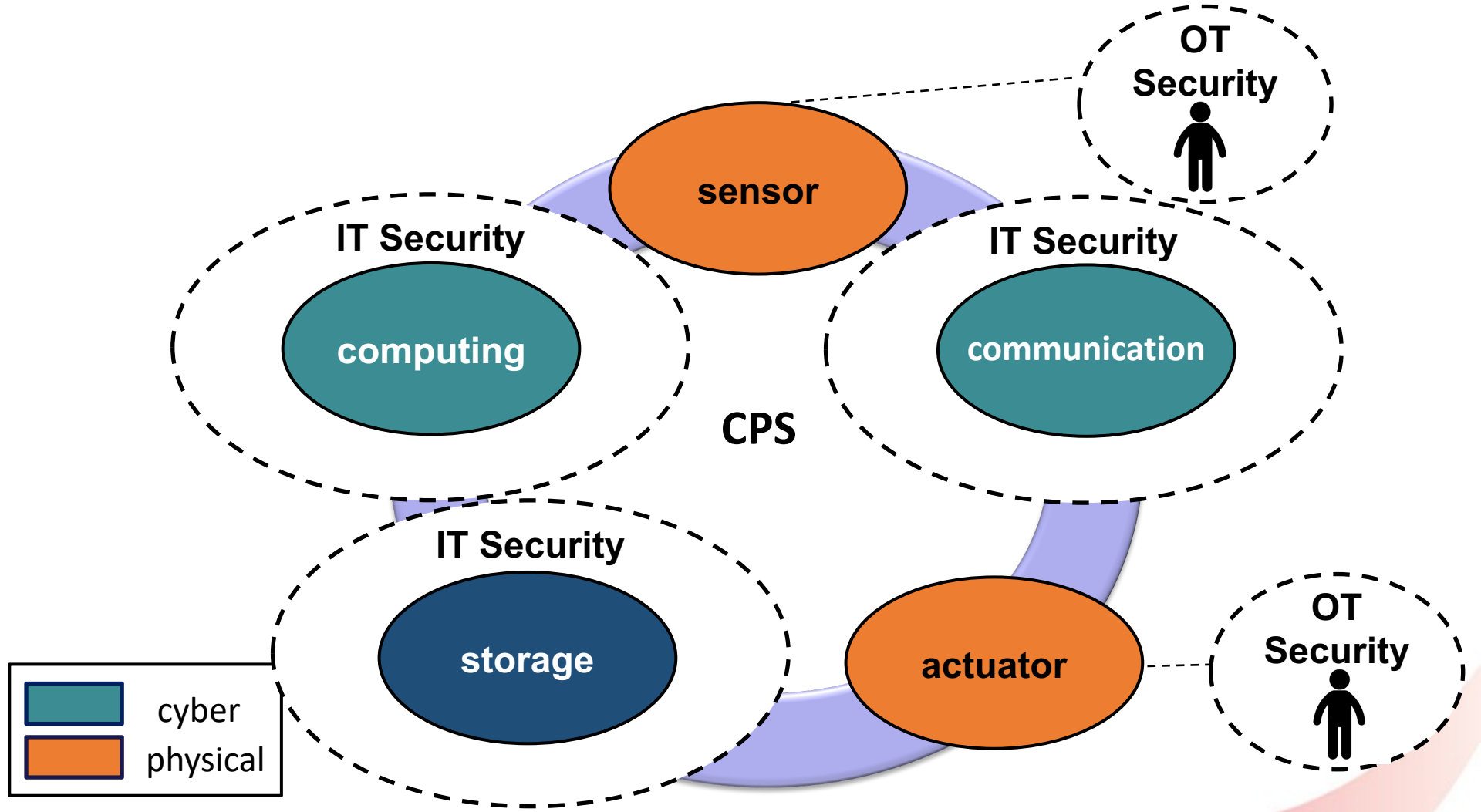


NANYANG TECHNOLOGICAL UNIVERSITY

AV Attack Surfaces

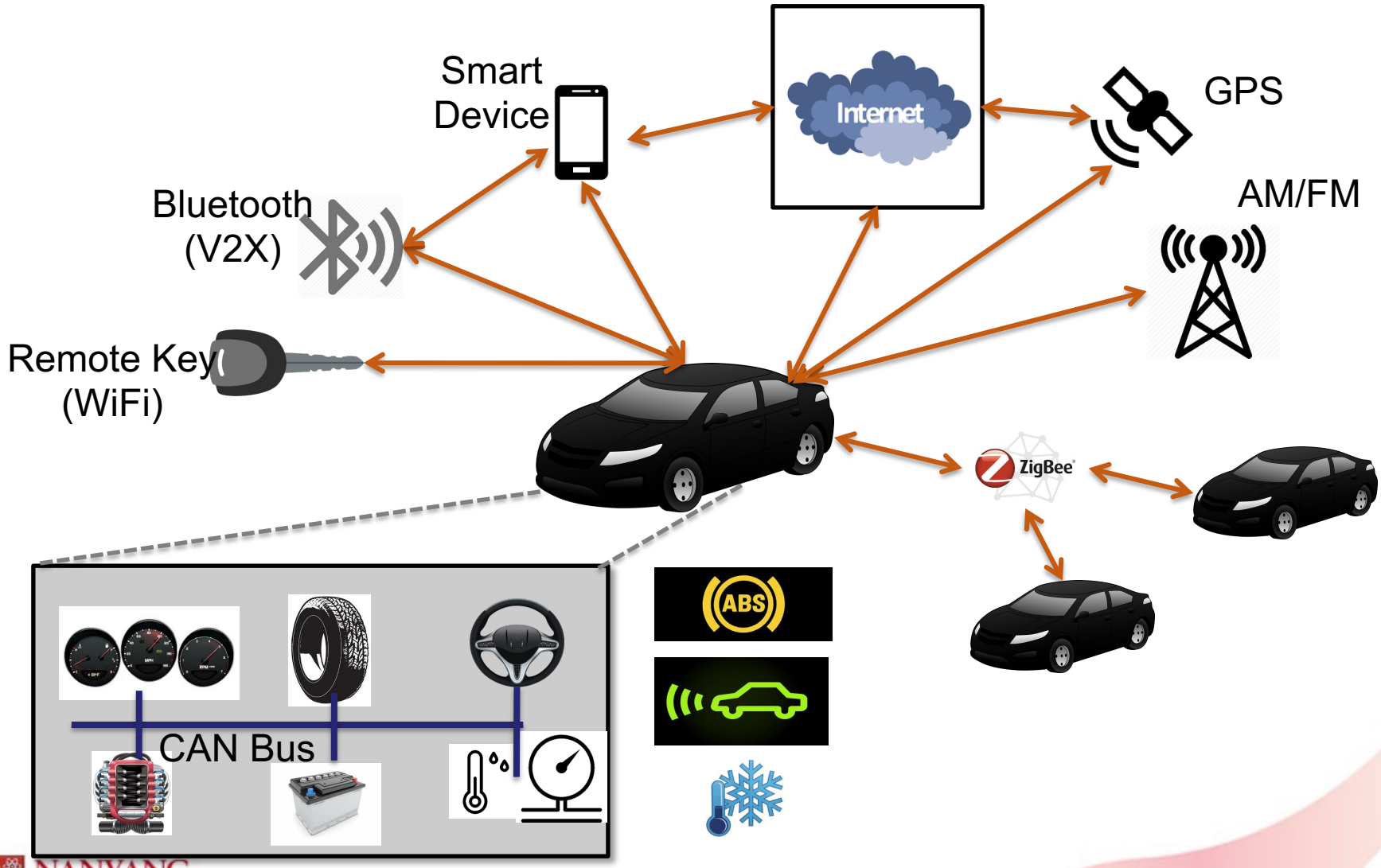


AV as CPS

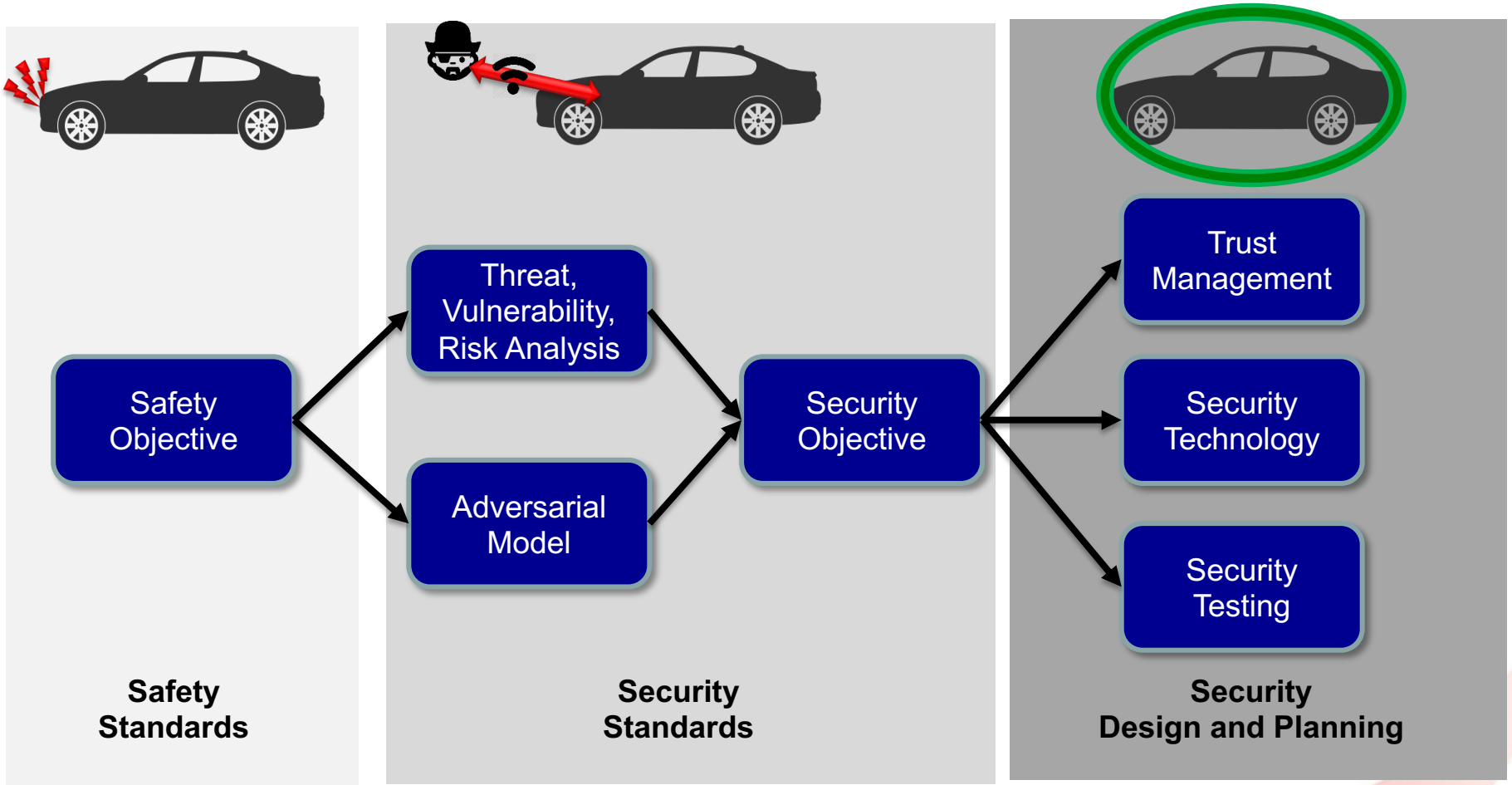


NANYANG TECHNOLOGICAL UNIVERSITY

AV as IoT

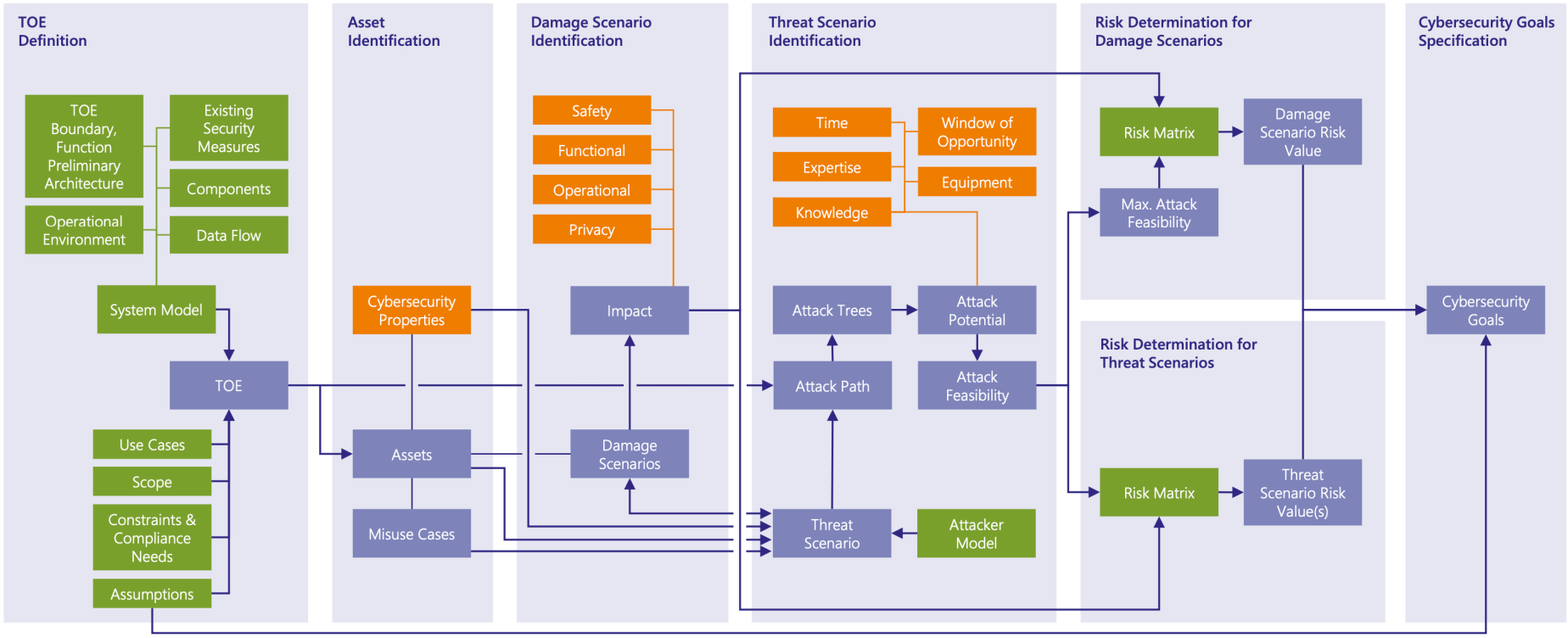

Smart Device
Internet
GPS
Bluetooth (V2X)
AM/FM
Remote Key (WiFi)
ZigBee
CAN Bus
ABS

AV: Safety to Security



NANYANG TECHNOLOGICAL UNIVERSITY

Threat Analysis and Risk Assessment (TARA) model



TOE: Target of Evaluation

NANYANG TECHNOLOGICAL UNIVERSITY

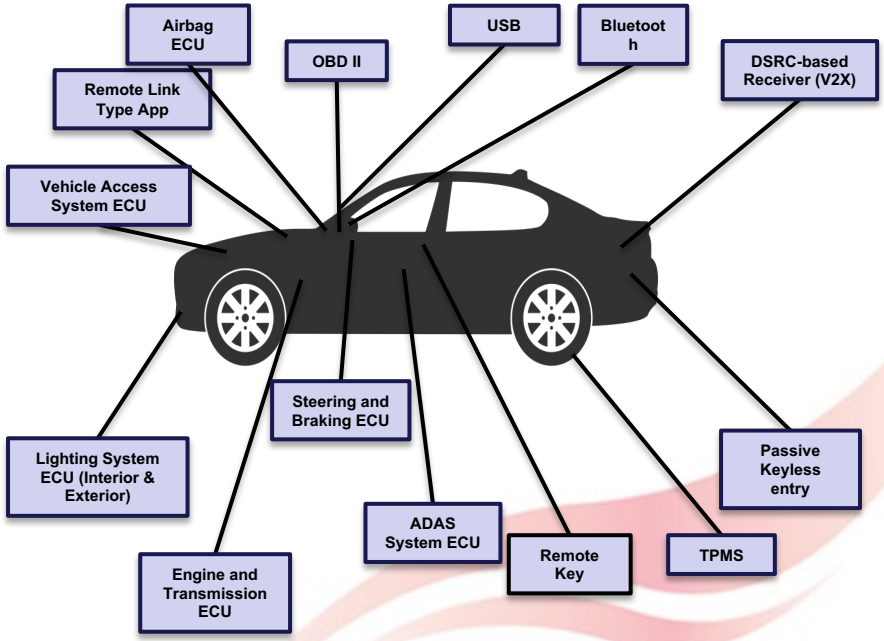
Contents

- Automotive Security Incidents
- Attack Models and Standardization
- Security by Design
- *Discussion*

NANYANG TECHNOLOGICAL UNIVERSITY

What did we learn?

- Modern automotive is surprisingly easy to attack
  - Dominantly mechatronics
  - Systematic security analysis is evolving
  - Limited understanding of modern IoT/CPS/IT attacks
  - Critical for Autonomous Vehicles
- Security Incidents Analysis
- Security by Design



NANYANG TECHNOLOGICAL UNIVERSITY

The End

NANYANG TECHNOLOGICAL UNIVERSITY