

# Parallel Universes? Contrasting CAN Bus Security in Automotive and Space Domains

Marcio Juliato



# Notices & Disclaimers

Intel technologies may require enabled hardware, software or service activation.

No product or component can be absolutely secure.

Your costs and results may vary.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

The products described may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

© Intel Corporation. Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of others

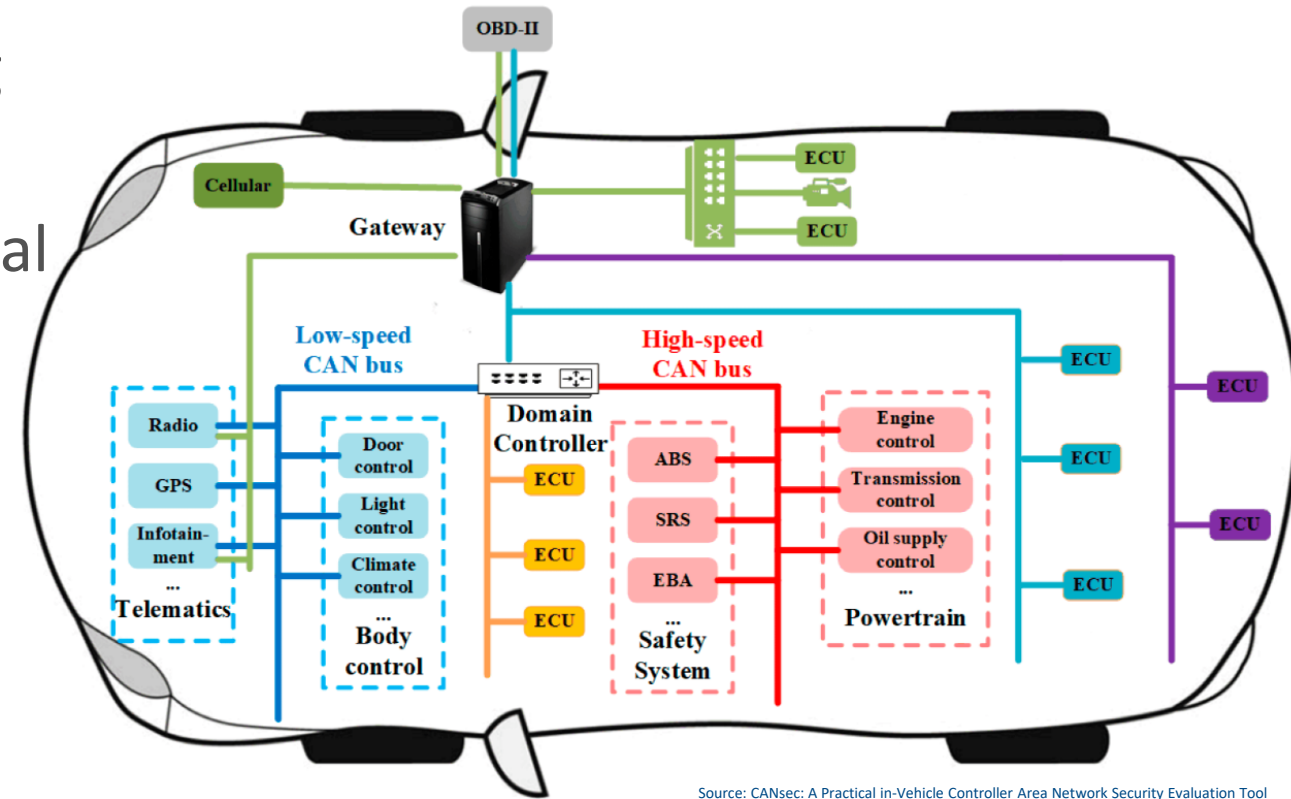
# Outline

- CAN Bus Intro
- Common Attacks
- Threat Landscape
- Discussion of Space vs Automotive Environments
- Some Security Approaches
- Conclusions



# CAN Bus in Automotive

- Controller Area Network (CAN) is a de-facto network in current and upcoming vehicles
- Provides high reliability for safety-critical functions
- ECUs carry out their tasks through reception and broadcast of messages
- Hundreds of ECUs; Several interconnecting buses, including with other networks and external connectivity
- Large attack surface

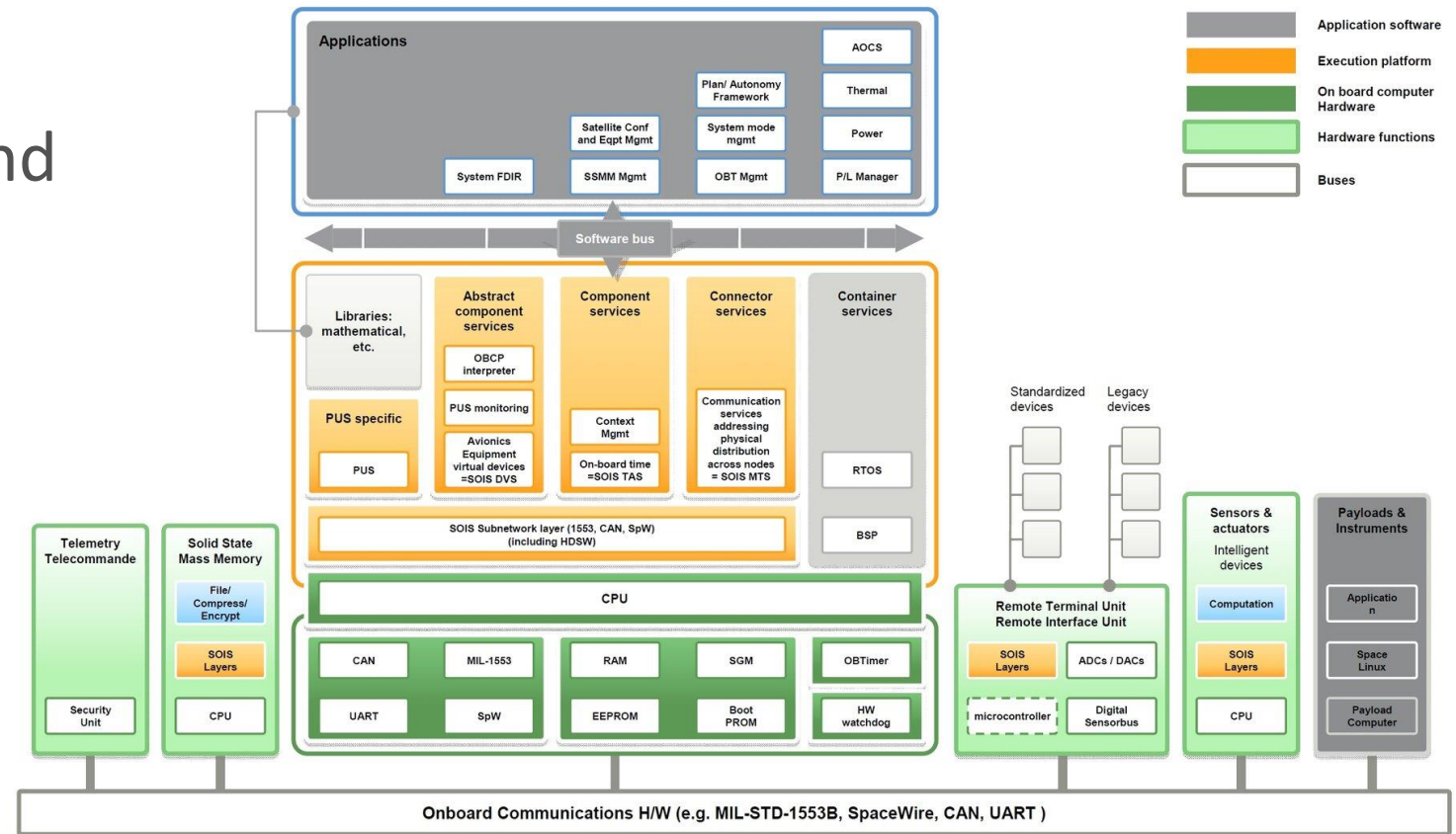


Source: CANsec: A Practical in-Vehicle Controller Area Network Security Evaluation Tool

CAN Bus Architecture

# CAN Bus in Space

- CAN bus is being standardized by ESA and the ECSS
  - Covered by ECSS-E-ST-50-15C
- Used for internal command and control buses
- Generally less interconnected components
- Relatively less exposure than Automotive (more on that later)



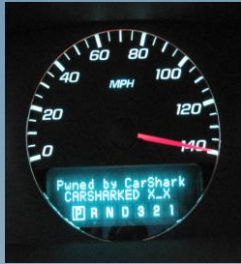
Onboard Data Systems Architecture

Source: ESA

# Some Limitations

- Lack of built-in data origin authentication
- Constraints in bandwidth
  - Use of authentication messages is hard due to network bandwidth and load
- Crypto techniques would bring the associated latencies, key management issues, etc.
  - Does not prevent internal attackers from transmitting authenticated malicious messages

# Attack Landscape



Compromised Instrument Panel 2010



Jeep 2015



Tesla 2017



Tesla 2016



BMW 2018



Bosch Drivelog 2017



Lexus/Toyota 2020

**Automotive cybersecurity incidents doubled in 2019, up 605% since 2016**

Upstream 2020 Cybersecurity Report

**2020 UN Regulations for Vehicle Cybersecurity Approval**



April 1986

**Satellite attack: the mounting arms race in space**



November 2021

**The ingredients for ransomware attack in space are here - interview**

by Vilus Petkauskas © 03 March 2022

**HK probes Falun Gong 'hacking'**

By Chris Hogg BBC, Hong Kong

Hong Kong authorities are investigating after TV programmes beamed into China from the territory by satellite were allegedly hacked into at the weekend.



November 2004

**U.S. Satellites Are Being Attacked Every Day According To Space Force General**

Space Force general details how jamming, blinding lasers, cyber attacks, and other satellites have America's space-based capabilities under siege.

BY JOSEPH TREWTHICK NOV 30, 2021 10:00 PM

November 2021



III.1 ROSAT (1998)  
Hackers based in Russia took control of the U.S.-German X-ray science satellite ROSAT on 20/09/1998 in an example of an attack made via a satellite ground station. In this particular case, computers at the NASA Goddard Space Flight Center in Maryland were hacked before the hackers instructed the satellite to turn towards the sun. This effectively fried the satellite's batteries and optics, rendering the satellite useless [5] [17]. It was also reported that ROSAT data obtained in the attack was sent to Moscow [18].

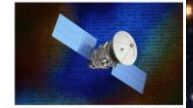
September 1998



March 1999

**An old satellite was hacked to broadcast signals across North America**

The demonstration reveals the vulnerability of decommissioned, but not dead, satellites.



April 2022

III.2 Landsat 7 (2007, 2008)  
On 20/10/2007 the U.S. earth observation satellite Landsat 7 jointly managed by NASA and the U.S. Geological Survey experienced 12 minutes of interference in an example of a direct attack on the satellite C2 link. The interference was only discovered following a similar event on 23/07/2008. Both attacks are thought to be attributable to China, however in both cases the responsible party did not achieve all the steps necessary to command and control the satellite [5] [16].



October 2007



III.3 Terra EOS AM-1 (2008)  
The NASA earth observation satellite Terra EOS AM-1 experienced 2 minutes of interference on 20/06/2008 and 9 minutes of interference on 22/10/2008. In both cases the responsible party achieved command and control of the satellite, however no commands were issued. The attacks were again attributed to China [16]. Although the attacks initially appeared to have come via the Kongsberg Satellite Services ground station at Seabast, the facility's owners saw no evidence of this and it may therefore have originated as a direct attack on the satellite C2 link [5].

June 2008

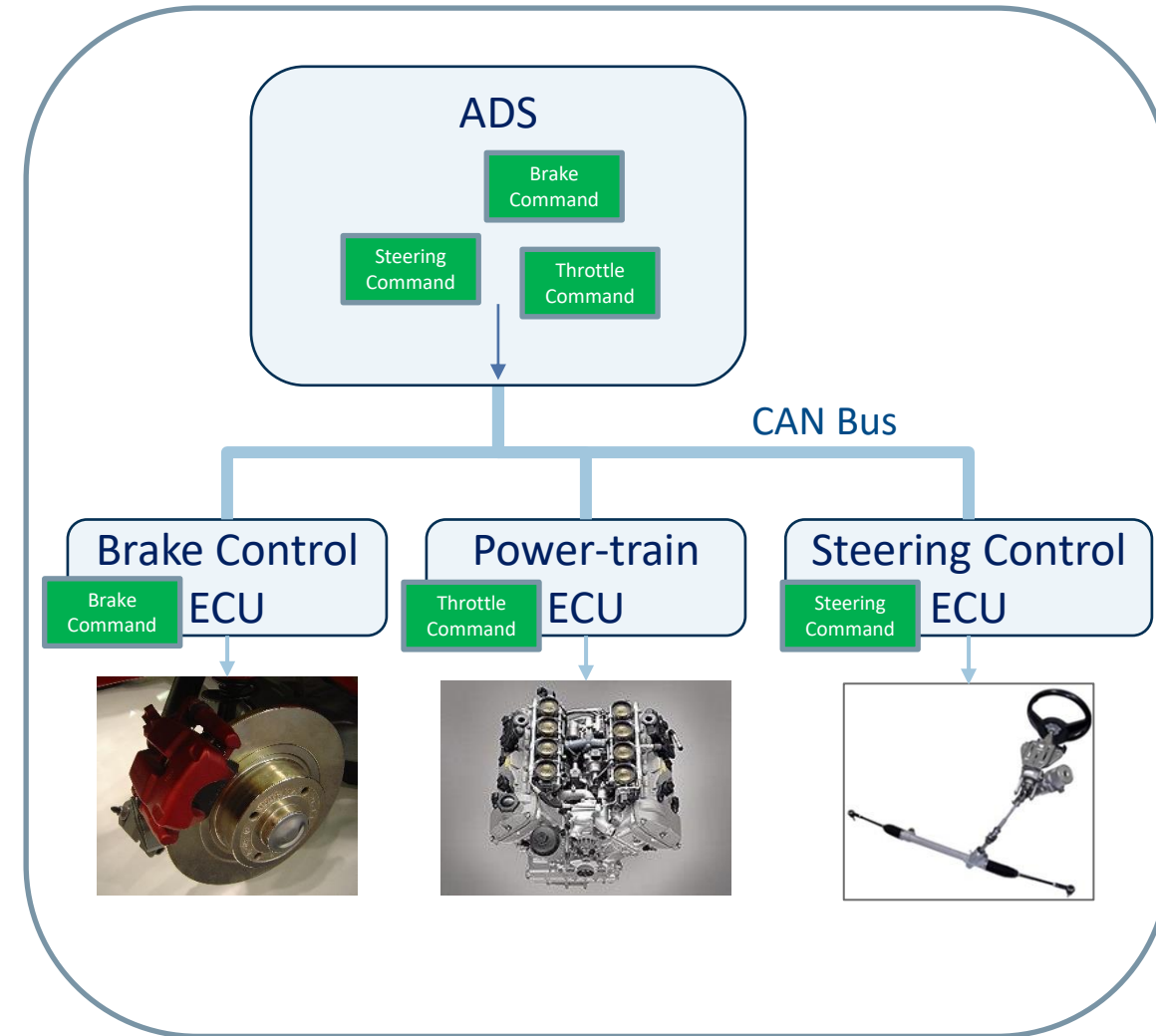


# Common Attacks against CAN Bus

- Masquerade Attacks
- DoS (Bus-off) Attacks

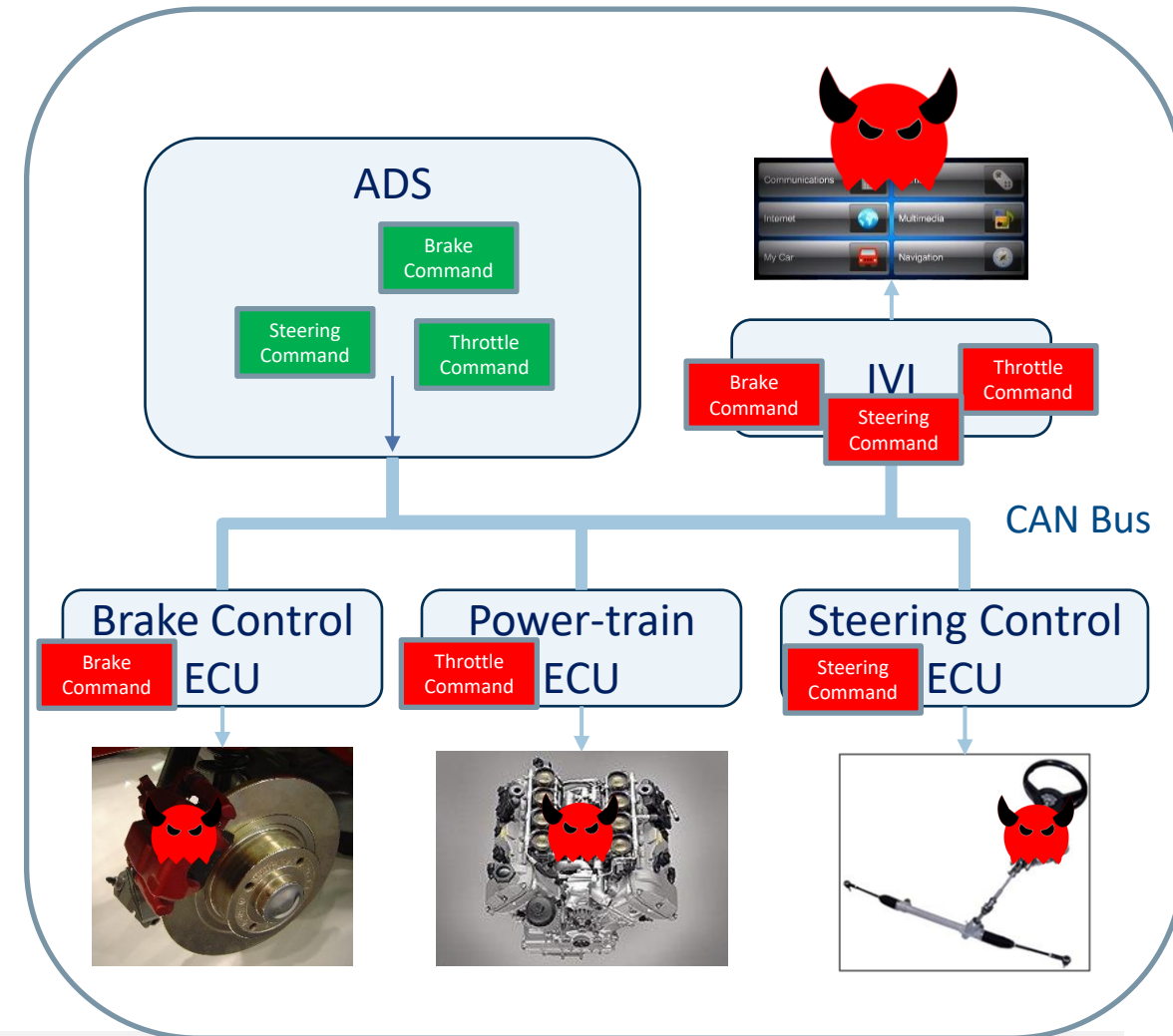
# Automotive Example - Actuation

- Autonomous Driving System (ADS) interfaces with the CAN bus to actuate upon the vehicle
- ADS sends control commands to accelerate, brake and steer the vehicle
- Electronic Control Units (ECUs) receives commands and translates them into physical actions
- Similar control architecture and functionality onboard of spacecrafts



# Masquerade Attack

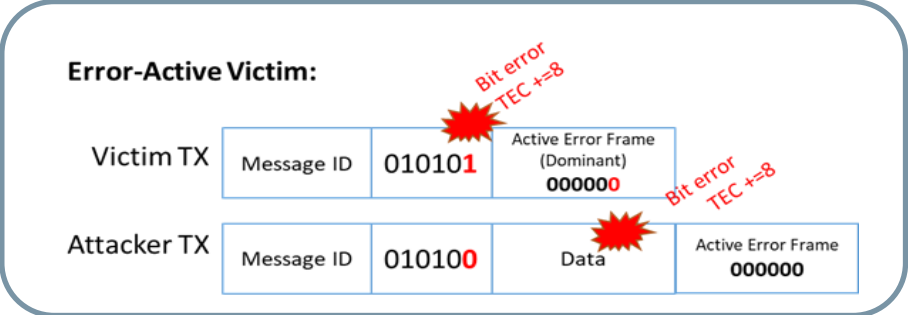
- Attacker gains access of a node (e.g., IVI\*)
- Malicious node transmits message identifier (MID) belonging to ADS
- Attacker can fully control the vehicle on behalf of ADS



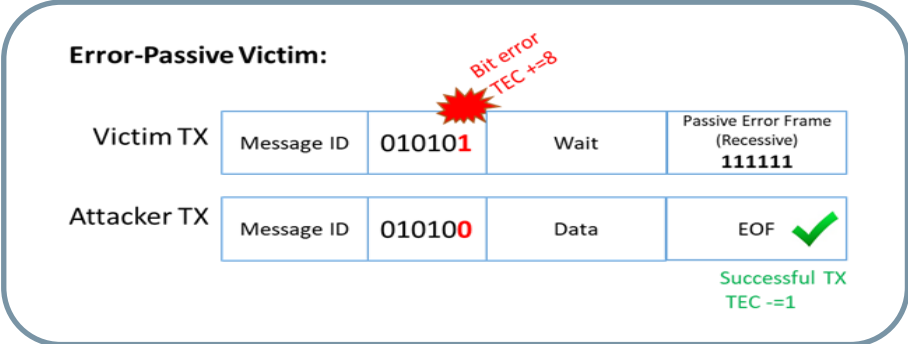
\*IVI: In-Vehicle Infotainment

# Bus-Off Attack

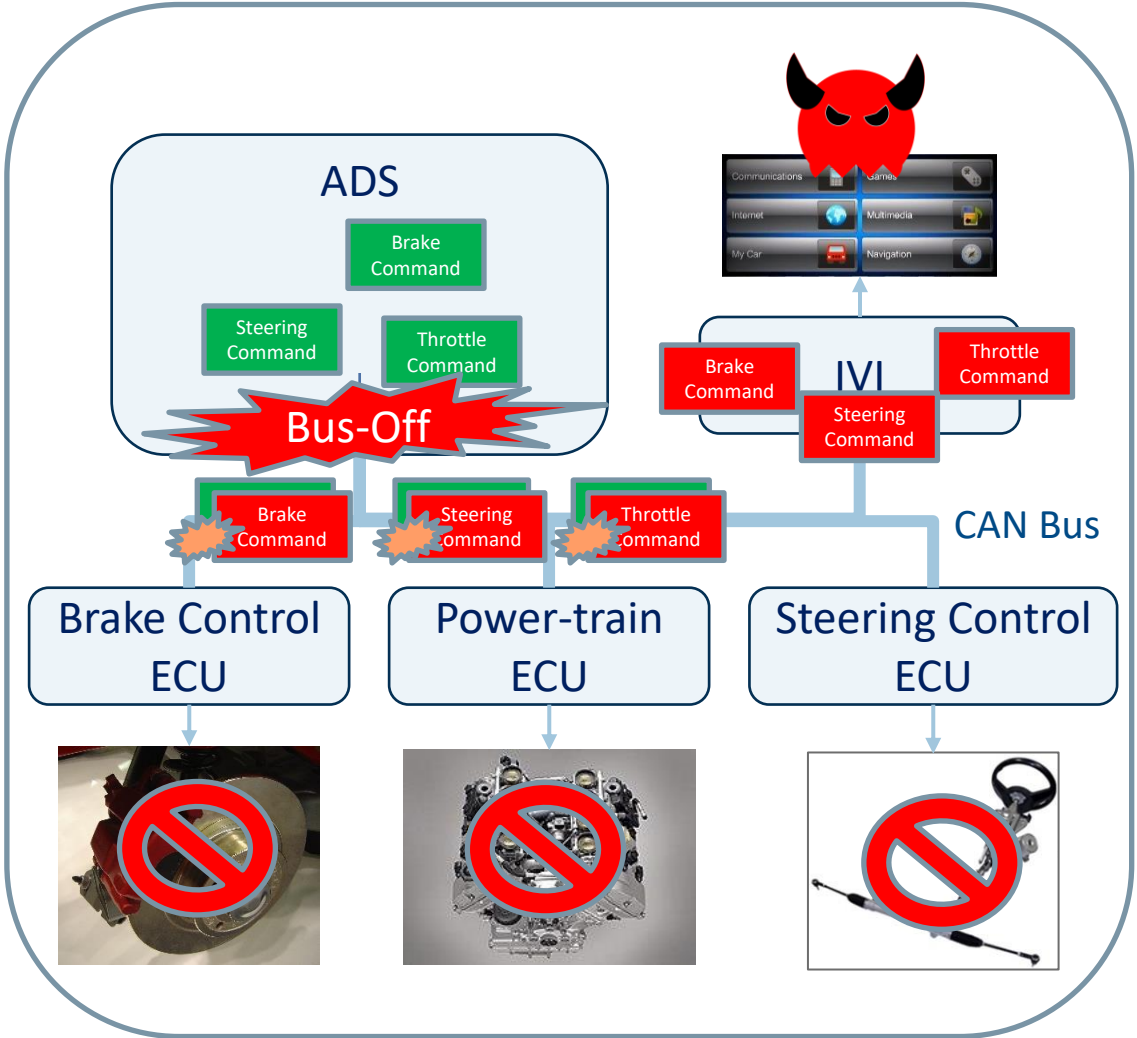
- CCS'16 paper [Cho et al.] introduced bus-off attacks
- Attacker causes controlled collisions to disconnect ADS from CAN bus



Victim and attacker accumulating errors due to the collisions



Victim entering bus-off, while attacker remains active with a successful transmission



# Particularities: Automotive

- Local and global threat exposure
  - Physical tampering, including direct access via OBDII port
  - External connectivity via Wi-Fi, Bluetooth, cellular, V2X
- 100's of ECUs from different manufacturers
- Several co-existing in-vehicle networks
  - CAN, LIN, FlexRay, Ethernet, etc.
- Security solution design constraints:
  - Real-time response and accuracy are critical
  - More relaxed power budget
  - Higher processing capabilities
- Can be brought to a garage for maintenance
- Average age of automobiles in USA: ~13 years\*



OBDII port allow direct access to CAN buses

Source: Kaspersky

\* Bureau of Transportation Statistics 2023

# Particularities: Space

- Global threat exposure
- Physical attacks possible pre-launch, but infeasible post-launch
- Less components from a lesser number of manufacturers
- Relatively small number of components and networks onboard
- Much more constrained environment (power, computational capabilities)
  - Constrains the design space of possible security solutions
- So far, we still don't have a garage in space for maintenance 😊
- Longer lifespan
  - Telecom satellites: 10-15 years
  - International Space Station (ISS) (1998): 25 years
  - Hubble (1990): 34 years
  - Voyager (1977): 47 years
    - Diffie-Hellman paper published in Nov 1976

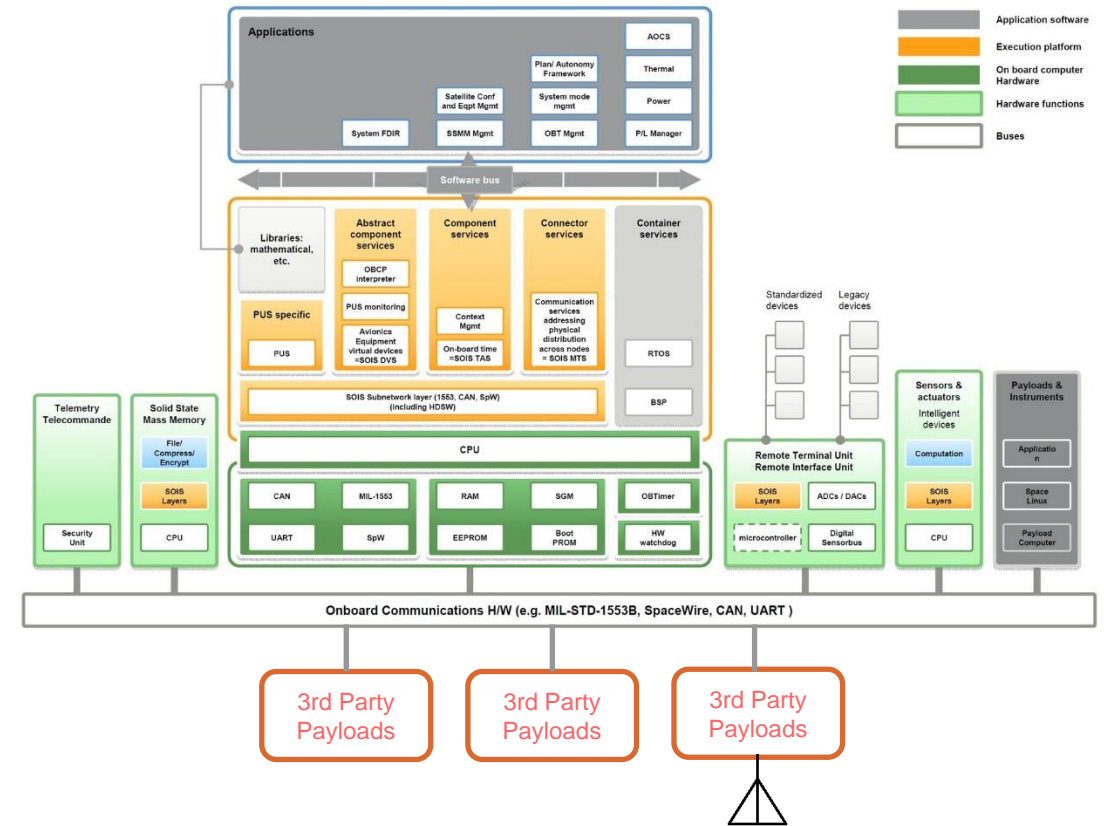


Source: NASA

Voyager spacecrafts: launched in 1977, currently 14.48 billion miles from Earth

# Commonalities

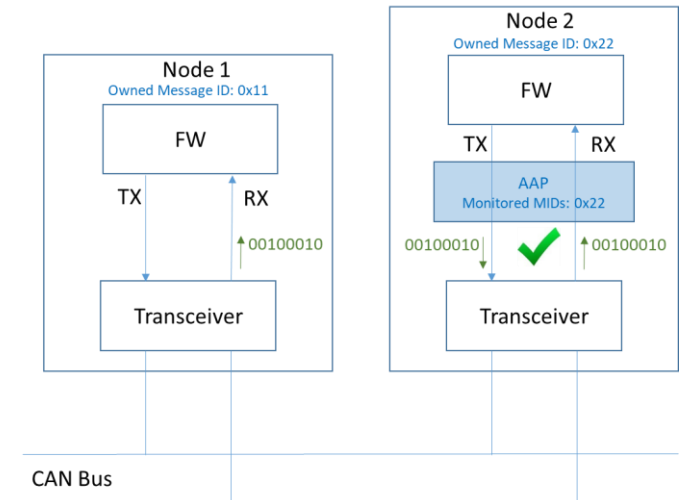
- Real-time systems demanding ultra-low latency of security solutions
- KISS (*“Keep it simple, stupid”*) type of security solutions
  - Complex mechanisms are usually “no-go”
  - Minimal requirements
  - Transparent operations
- External connectivity as entry points for attacks
- Ever-expanding attack surface
  - Especially when hosting 3<sup>rd</sup> party payloads



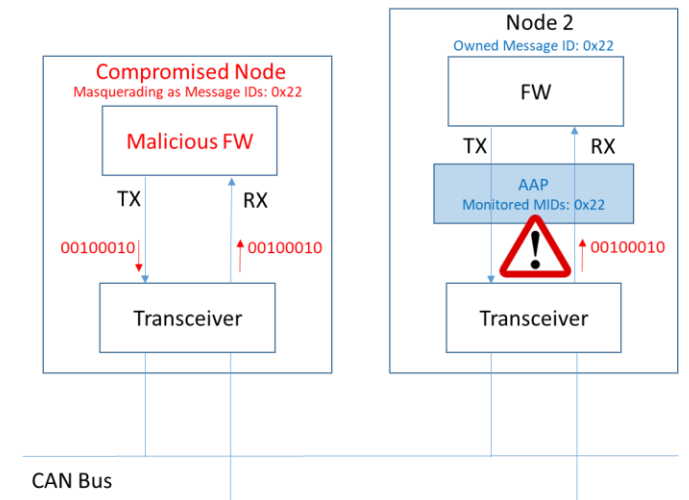
Expansion of attack surface through hosted 3<sup>rd</sup> party payloads

# Real-Time Masquerade Attack Detection and Prevention

- Protect system from impersonation on the CAN bus
- Strategy: Continuous bus monitoring from the perspective of the protected ECU
- Detection of message in the bus owned by the protected ECU when it has not transmitted it
- Remedial action to neutralize the message in real-time
- Avoid consumption of malicious message by the remaining of the system



Authentic conditions

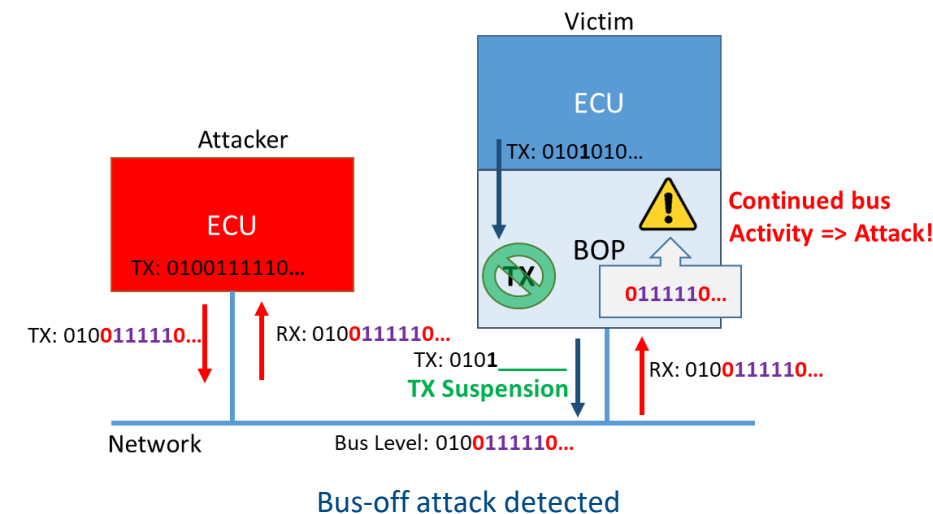
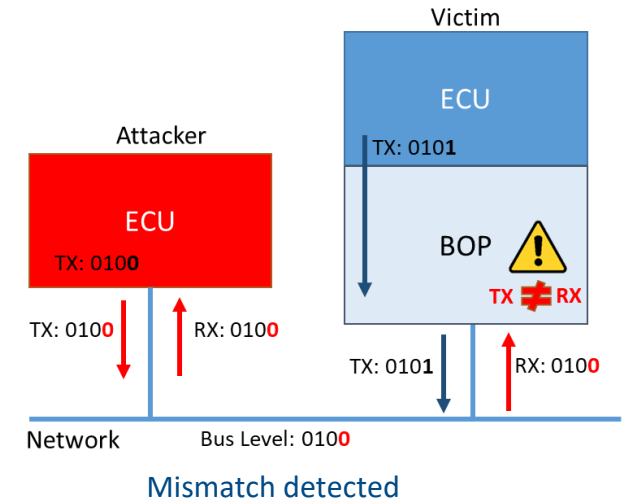


Masquerade attack detected



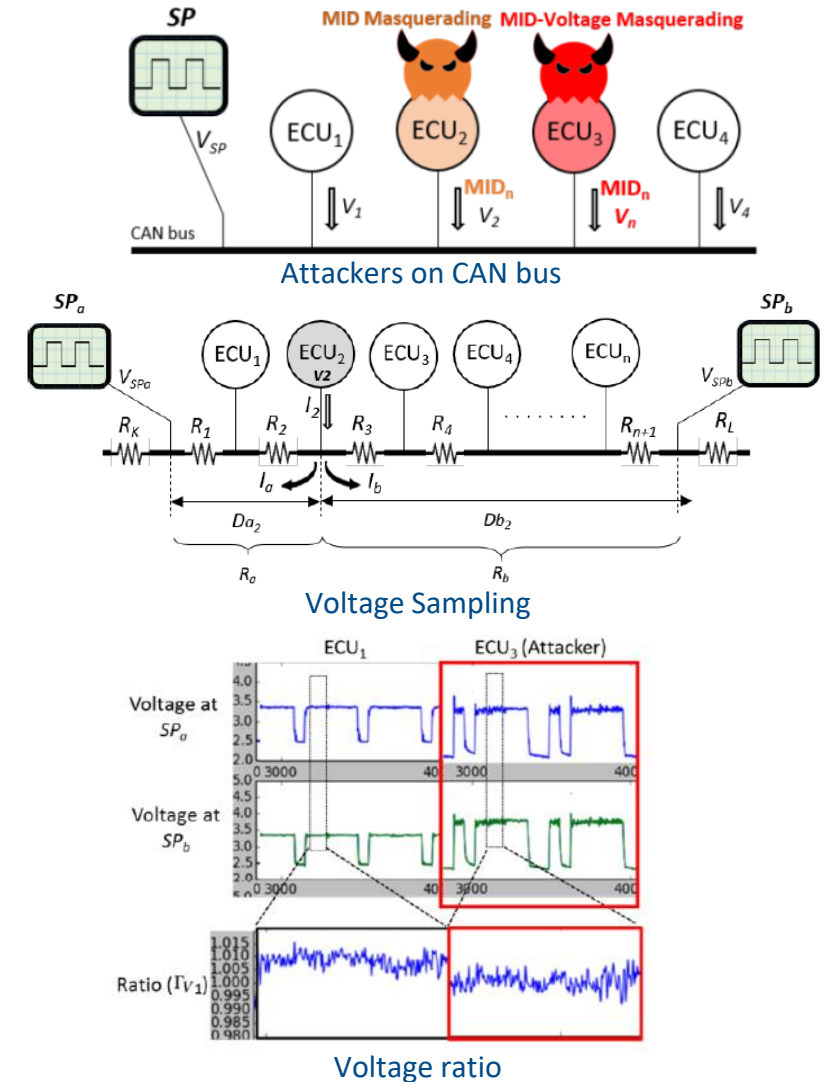
# Real-Time Bus-Off Attacks Detection and Prevention

- Strategy: Not immediately to follow the attacker-induced fault-containment protocol. Rather, differentiate between faults and attacks.
- Detect bit mismatches, temporarily suspend further transmissions of the protected node
- Determine whether bit-mismatch was caused by a fault or attack
- Revert bus-off attack against the attacker
  - Bit corruption of the attacker's messages



# Masquerade Attack Detection through ECU Voltage Fingerprinting

- Focus on masquerading attacks
- Traditional Message Identifier
- Message Identifier+Voltage Masquerading
- Strategy: Prevent masquerading by profiling voltages of transmitting ECUs
- Two voltage sampling points
- Physical location of the ECUs determines specific voltage ratios at the sampling points
- Attacker unable to forge voltages to satisfy both points simultaneously
- Overall F1-score: 99.4%



# Summary

- CAN Bus is widespread and reliable but presents several security challenges.
- Real-time and performant security solutions are hard to build.
- Automotive and Space domains have their own particularities but share a number of commonalities that must be addressed when building a secure system.
- Automotive presents a larger attack surface, in which ML and HW-based solutions can be effective to counteract attacks in real-time.
- Spacecrafts require careful consideration of the expanding threat surface due to 3rd party payloads and may require more efficient solutions due to onboard constraints.

Thank You!