Tomorrow’s Data Storage Integrity and Safety for Autonomous Cars

Dealing with Security, Safety and Reliability

Bernd Niedermeier, Tuxera Inc.
Automotive Systems Today and Tomorrow

Flash Memory Summit 2019
Santa Clara, CA

30 to 100+ ECUs
Flashed once, minor updates
Predefined/fixed use case
Closed system

6-10 area/domain controllers
Separated partitions by function and tier1 / OEM
OEM Apps / new services
Open system

6-8 operating systems
Considered read only
Flash write not an issue
Power Supply, Cost

Hypervisor + 1 - 4 (RT)OS
Android -> new use cases
Always online, OTA updates
Flash write an issue

Flash Memory Summit 2019
Santa Clara, CA

2

Flash Memory Summit 2019
Santa Clara, CA

2
Data to be processed...

1 GB/s sensor data
3.6 TByte per Hour
28.8 TByte per day

Event Data Recorder
legal requirement
constant write to Flash
Challenge #1, Reliability over Lifetime

What app will be running in 5 years from now?
How will it interact with the system and Flash?

New Apps, OTA Updates, EDR resulting into more write load for Flash

How to achieve 10-15 years lifetime for the system
How to “correctly” dimension the system
How to keep cost under control
Filesystems do have an impact
different studies suggests that Android can create WAF of >20 (!)
Fragmentation might degrade system performance to critical point
Fail safe operation highly important – avoid corrupted data

Examples
FCA reboot loop 02/2018 in Uconnect infotainment systems

Spotify Bug 11/2016 – writing 5-10GB / hour into Flash
https://arstechnica.com/information-technology/2016/11/for-five-months-spotify-has-badly-abused-users-storage-drives
Challenge #2, Cyber Security

Connectivity creates attack angles
WLAN, Bluetooth, 3G/4G/LTE...
High risk for OEMs: security issue becoming functional safety issue?
Security gaps have to be fixed via OTA updates

High focus at OEMs and tier1’s
Security still a rather new area – new structures vs. legacy IP
SW vendors receiving first requests for CVE Scan results and penetration testing
Challenge #2, Cyber Security

Filesystem contribution to security

- Secure boot – e.g. dm-verity
- Encryption via dm-crypt, fscrypt …
- Quota setting
- Hierarchical CRCs (Merkle-Trees)
- Other…
Challenge #3, Functional Safety

Well established approach – ISO 26262

“Analyzing the different ways a system can fail and handle those cases such that there is freedom of unacceptable risk of physical injuries.. (fail safe)”

ASIL-C and ASIL-D certified systems out there TODAY
  e.g. L2/3 ADAS -> ASIL-D; digital cluster -> ASIL-B/C

What about certified Flash Memory?
Challenge #3, Functional Safety

Only certain safety goals require ASIL-D
E.g. tell tales in digital cluster -> ASIL-C
Rest of system via QM (standard quality management)

Future is not clearly defined yet
Requirements not always known upfront – might change during project
Request for certified Flash?
Filesystems required to be certifiable towards ASIL-D as well?
Nice-to-have vs. mandatory?
Conclusion

Autonomous Cars and new ECU architectures creating new challenges
  Reliability over Lifetime
  Cyber Security
  Functional Safety Requirements

Impact of filesystems and capabilities often underestimated / unknown

Filesystem companies like Tuxera open to discuss new approaches
  Partner solutions, security, functional safety
Conclusion

There are standards, but not ONE single, correct approach
-> what solutions are really needed in the future?

Need for open and collaborative discussions between
Tier1’s and OEMs
HW component vendors
SW vendors
Tomorrow’s Data Storage Integrity and Safety for Autonomous Cars

How to deal with Security, Safety and Reliability

Bernd Niedermeier, Tuxera Inc.

Images on slides 2,6,7,11 from rawpixel.com