ETSI Security Week(ISE Workshop)
16 June 2017

Considerations on certificate distribution for hybrid V2X

So-young Kim

LG
Life's Good

Contents

CTO Dev. /Advanced Standard R&D Lab

Research and standardization of preceding technologies on next generation mobile comm. / broadcasting / media codec / IoT

LG (CEO)

Company

CTO

CFO

CHO ▪ ▪ ▪

Vehicle Components

- LCD Cluster
- AVM[1] & Park Assist
- AVN[2]
- Connected Vehicle
  - Telematics
  - V2X

Home Entertainment

Home Appliance

Mobile Communication

Air Conditioning & Energy Solution

R&D: 2 Labs, 7 Centers,

Advanced Standard R&D Lab

System IC R&D Center

Living&Energy R&D Center

Vehicle Component Tech. Center

SW R&D Center

Convegence R&D Center

Power Electronics R&D Center

B2B Solution R&D Center

LSR/UX R&D Lab

※ Overseas R&D Labs:
US (Zenith Lab, San Jose Lab, Silicon Valley Lab), Japan, China, India, Russia, Finland,

ASL : Advanced Standard R&D Laboratory

1) Around View Monitor 2) Audio Video Navigation

CTO Div. / Advanced Standard R&D Lab

Vision

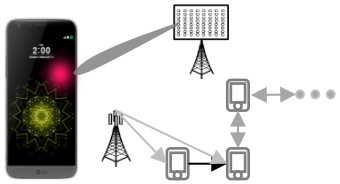
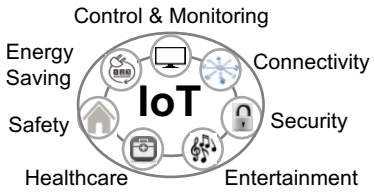
- **Become a global No.1 standard expert leadership on core technologies for future**

Mission

- **Research and standardization of preceding technologies on next generation mobile comm. / broadcasting / media codec / IoT connectivity**

Project

- **Standards-based PoC & solution development to lead newly emerging markets**

	Standard Body	Technology Map
Mobile Comm. 	• 3GPP LTE-A PHY/ Protocol/ Network/ Performance • 4G/5G Associations	• **LTE-A :** D2D, DC, CA, LTE-U, 3D MIMO ,Wi-Fi Interworking, MTC, Interference Cancellation ,V2X, Flexible Resource Allocation, Positioning • **5G :** Massive MIMO, LLR, FDR, New Waveform, New Multiple Access, mmWave
Vehicle, Broadcasting & Media 	• **ITS G5/WAVE V2X** • ATSC, DVB, HbbTV, CEA • MPEG, SMPTE, ITU-R • BDA, UHDA, UltraHD Forum	• **ETSI ITS, C2C CC, SAE :** Security, Architecture, GeoNet, MCO, Applications • **Broadcasting :** IP Hybrid and UHD 8K • **Codecs :** Video/Audio, HDR, WCG, HFR, Panorama • **Content :** Storage based media and Security
IoT Connectivity 	• IEEE 802.11, Wi-Fi Alliance • Bluetooth, HDMI, UPnP • OCF, oneM2M	• **IoT Connectivity :** PHY/MAC Layer, Interference Mitigation, Low Power Transmission, Network Topology, Network Security • **IoT Platform :** SW Architecture, Middleware, Ubiquitous Cloud, Middleware, Big Data, Sensor Networking, Context-Aware

IoT(Internet **o**f **T**hings), **HDR(H**igh **D**ynamic **R**ange), **HbbTV(H**ybrid **b**roadcasting **b**roadband **TV**), **DC(D**ual **C**onnectivity), **CA(C**arrier **A**ggregation), **MTC(M**achine **T**ype **C**ommunication), **V2X(V**ehicle to **E**verything), **LLR(L**ow **L**atency **R**adio), **FDR(F**ull **D**uplex **R**adio), **WCG** (**W**ide **C**olor **G**amut), **HFR(H**igh **F**rame **R**ate)

Security Considerations on Current V2X Safety Communication

- **Backgrounds**

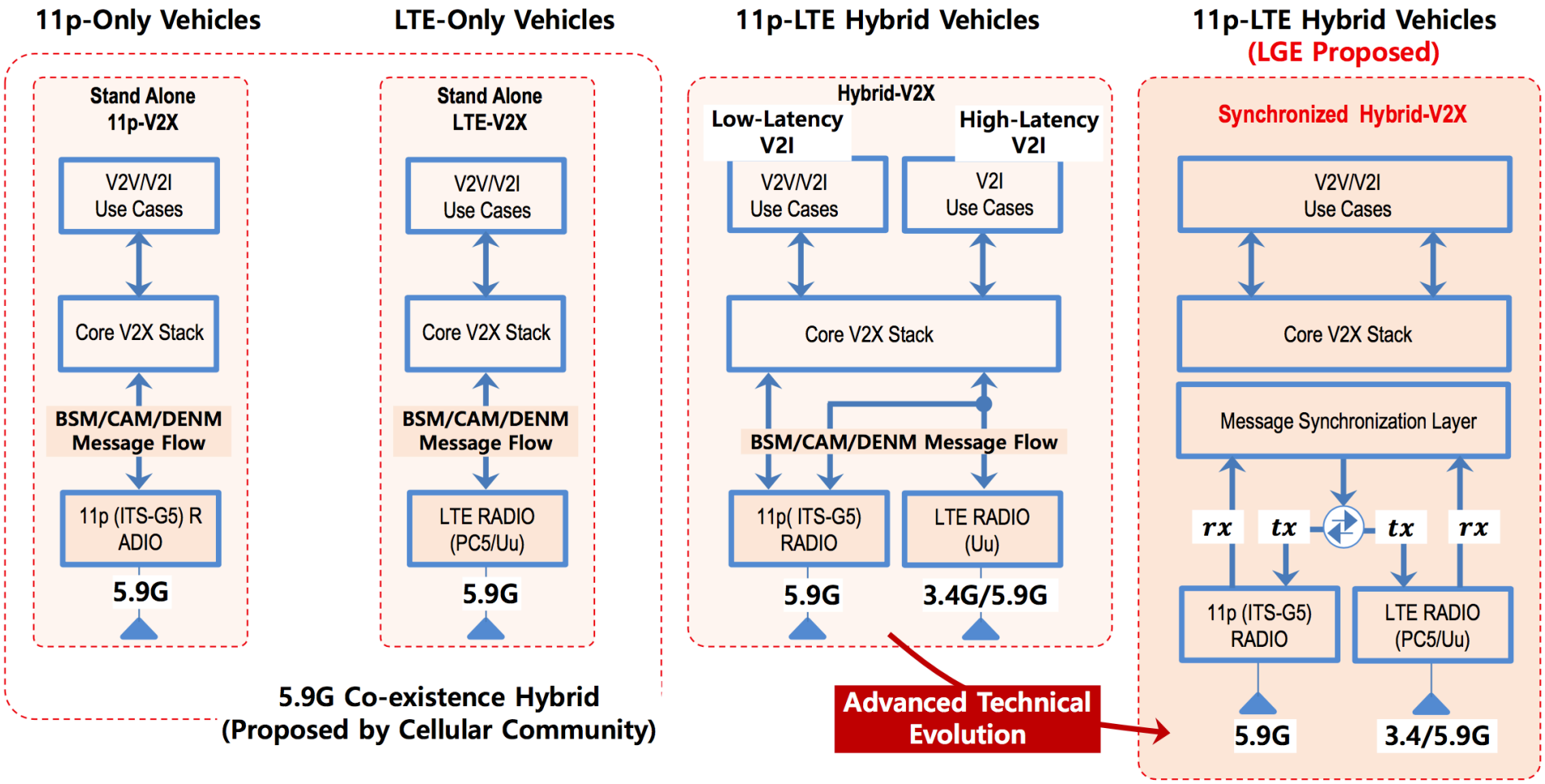
  - V2V Safety Communications is based on IEEE 802.11p(WAVE/ITS-G5) is currently proposed both in EU and US.

  - Other communication technologies such as 5G/ LTE/ Broadcasting/ Satellite etc. are also considered for V2V/V2I services.
    - LTE V2X services are proposing PC5, LTE-Uu Interfaces

- **Security Requirements on V2X Safety Communication**

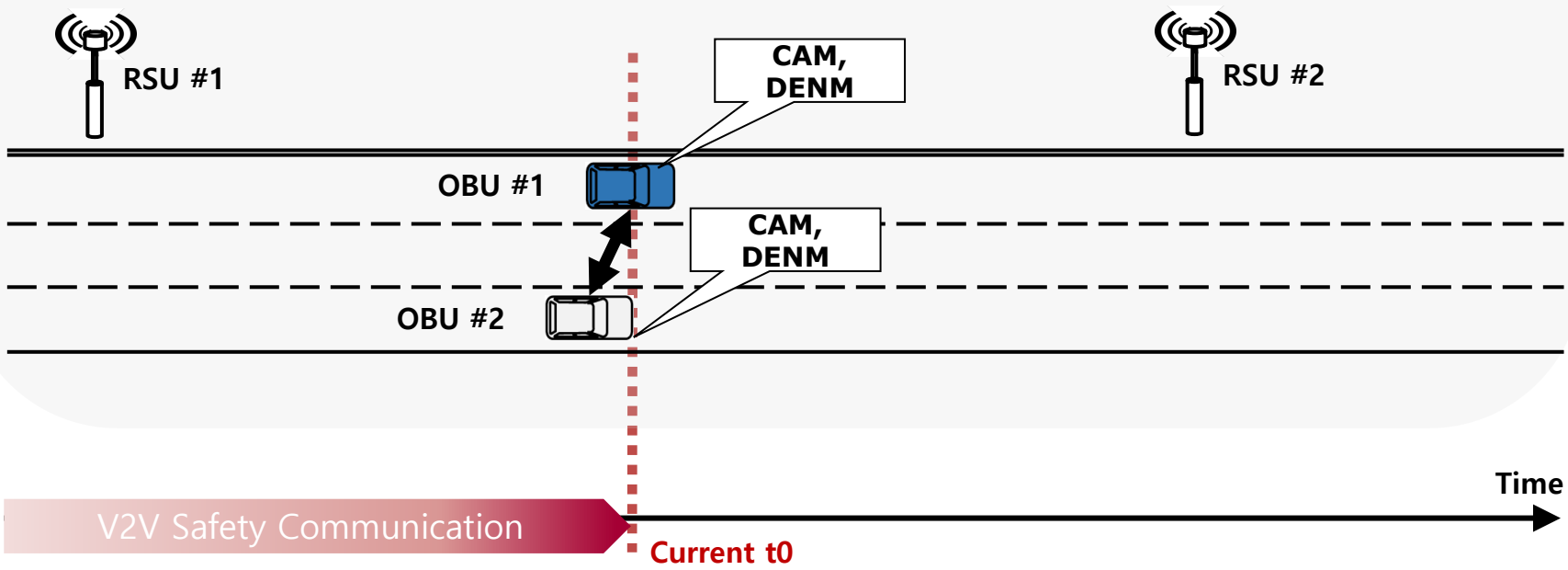
  - V2X Communication should guarantee that
    - Messages originate form trusted ITS stations
    - Messages are not modified during the transmission
    - Misbehavior ITS station should be detected and excluded from V2X communication

Possible Hybrid V2X Architectures



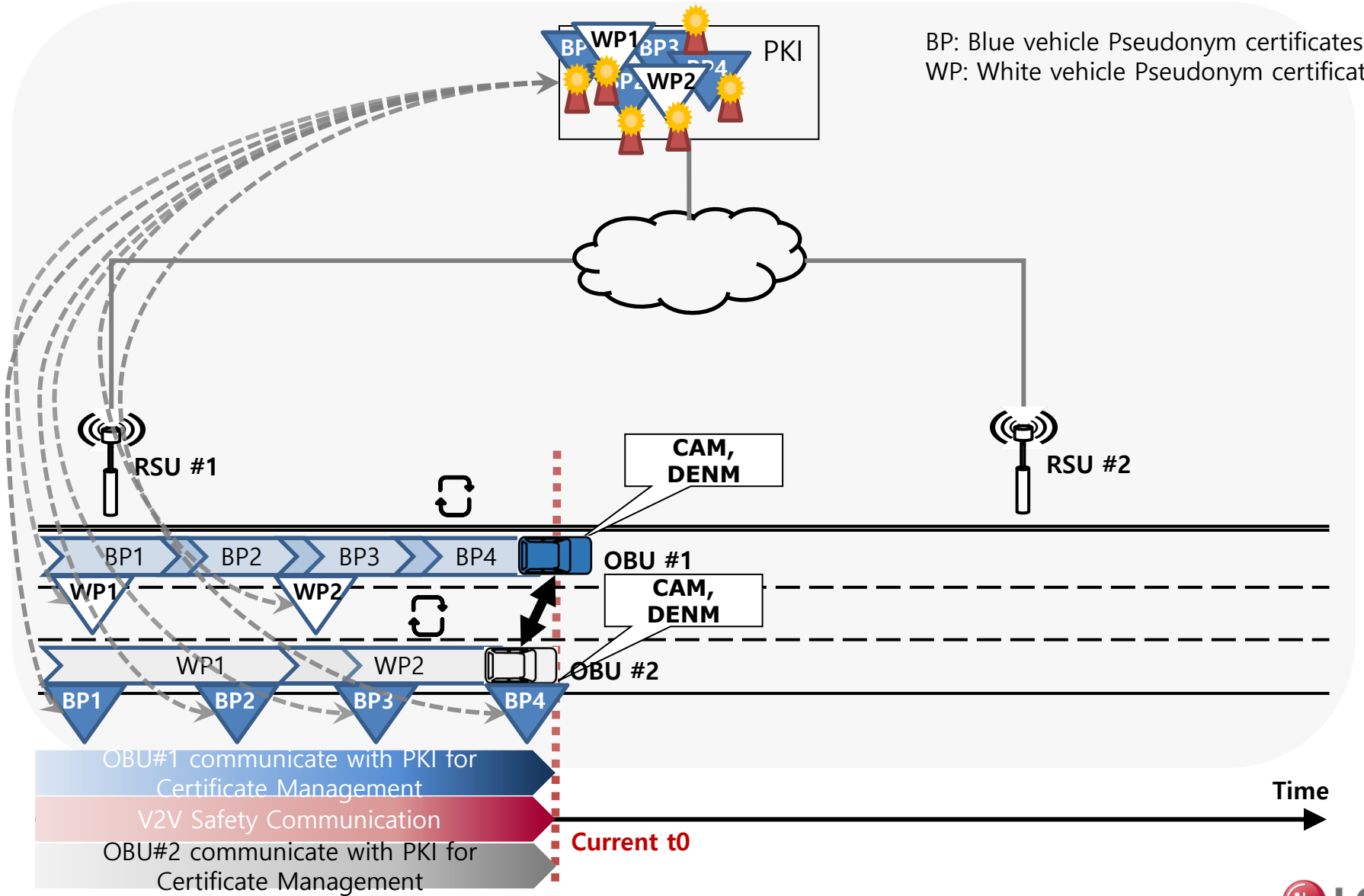
V2X Communication scenario on ITS G5

- It seems like that all ITS stations make CAM, DENM and communicate each other.



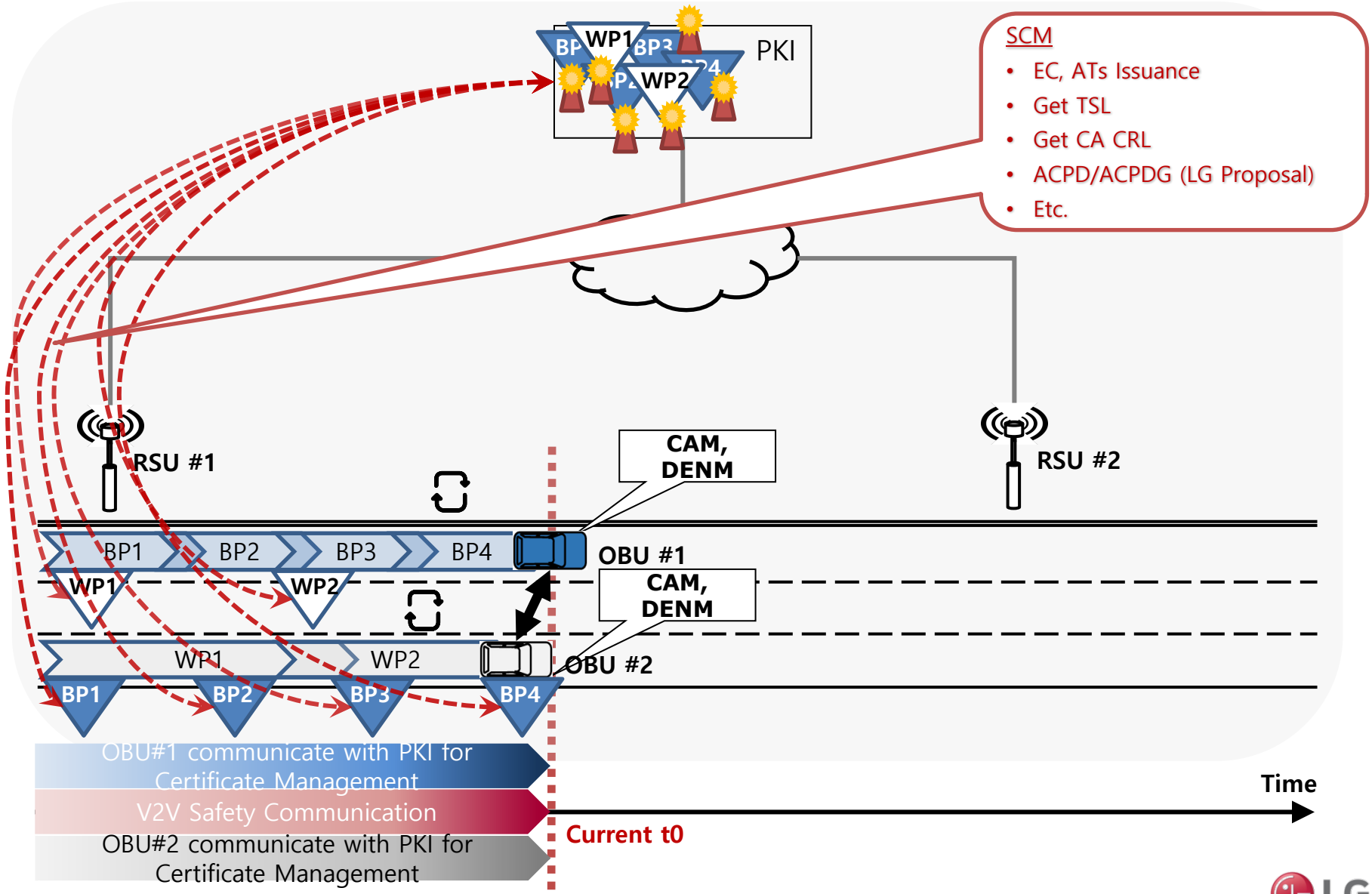
Vehicle to Vehicle Communication? Not only

- The minimal effort represented by PKI with Certificate Management



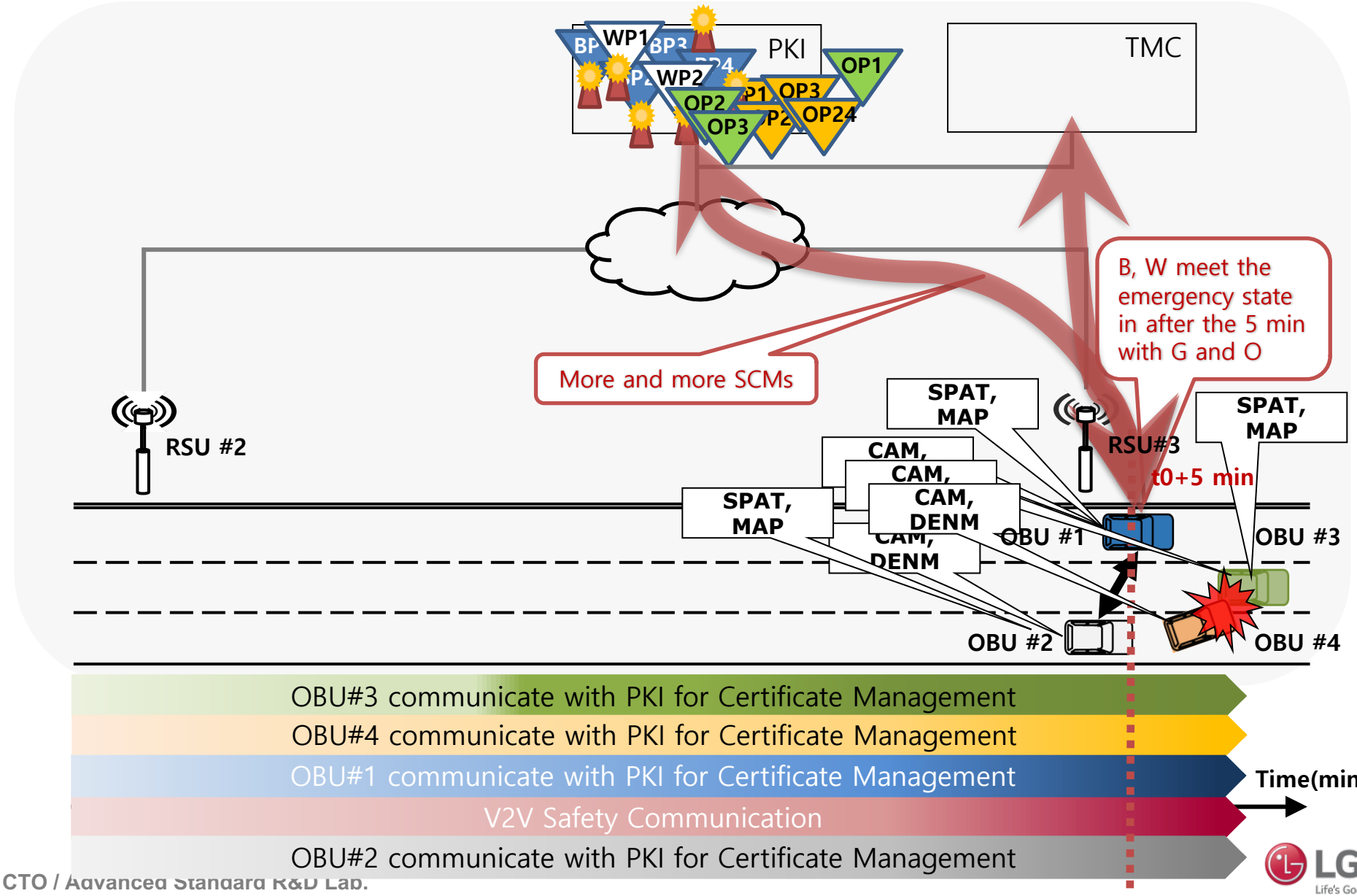
Security Credential Message(SCM) Definition

- SCMs are only for all kinds of security credential management messages via V2X communication.



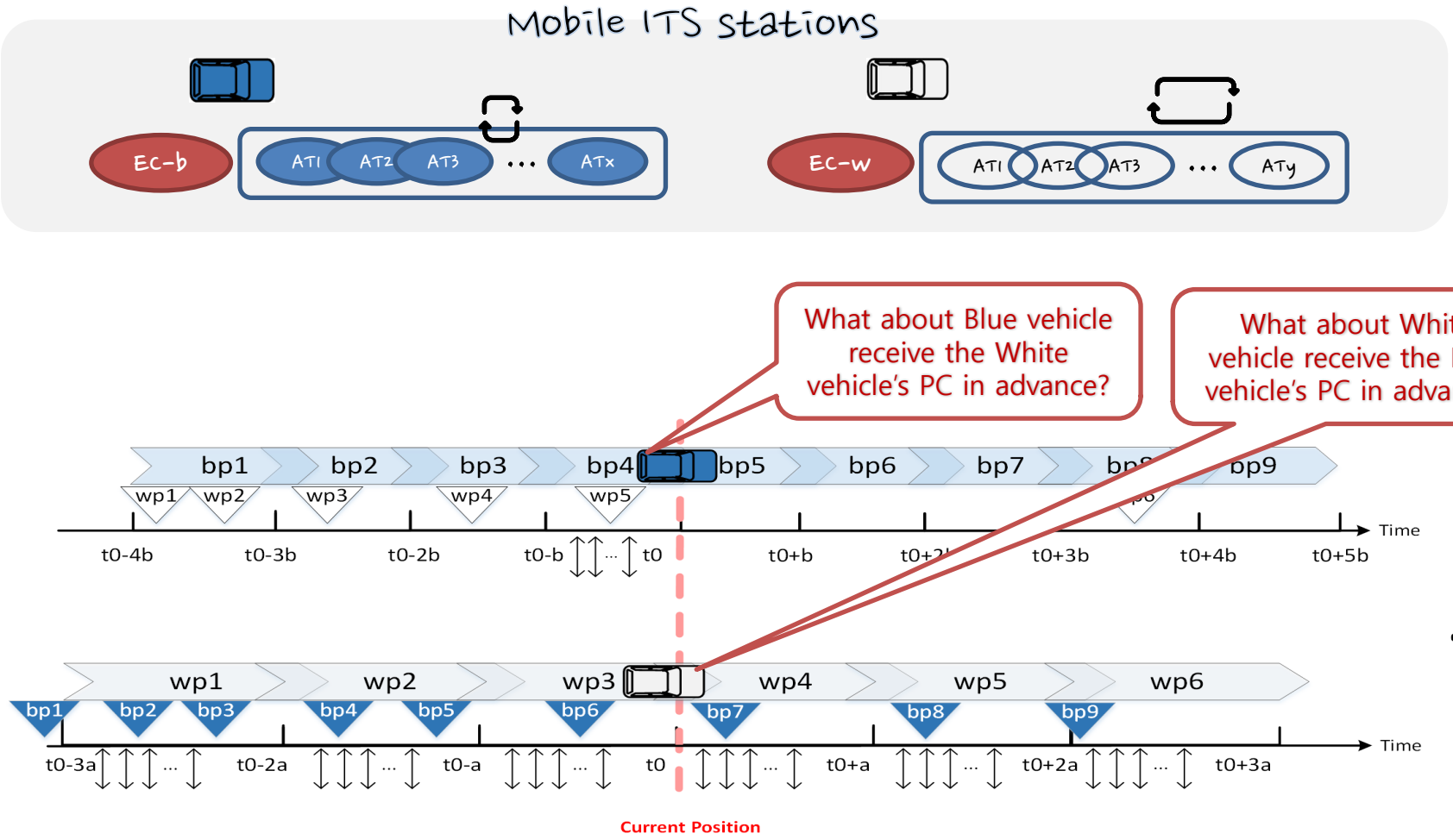
Necessary Mitigation from V2X message overhead

- There are plenty of various V2X messages and getting worse in case of congestion & emergency



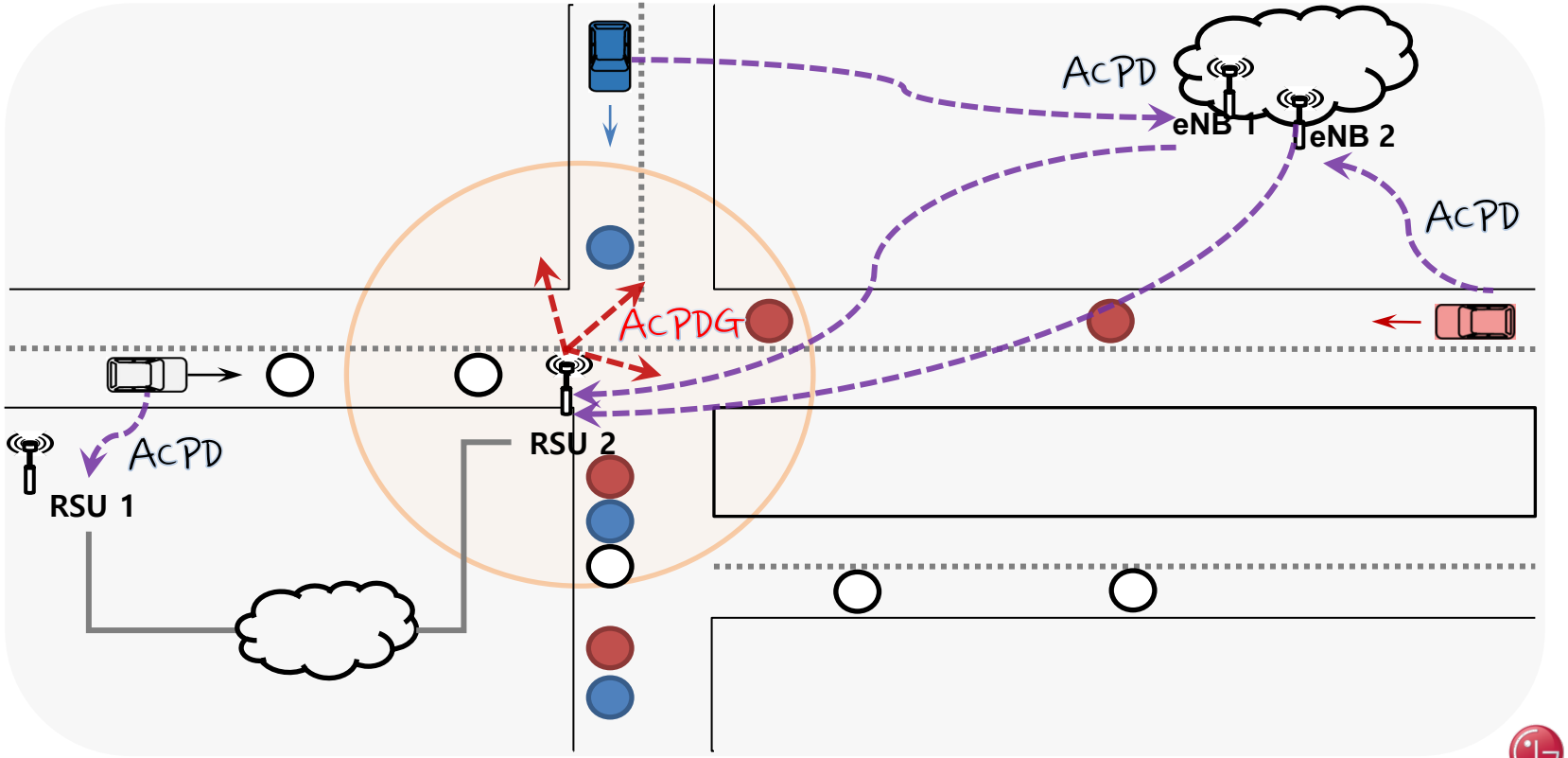
Get Ready for Future

- **Assumption**
  - All mobile ITS stations know their own destination and expected path
  - All mobile ITS stations has their own EC and ATs even though AT change policy and pool size if different.



Adaptive Certificate Pre-Distribution(ACPD) on Hybrid V2X

- Blue, Red, and White ITS-Vehicle Stations will meet at the scope of RSU 2 in 5 min.
- All ITS-Vehicles B, R, and W send ACPD Message eNB 1, eNB 2, RSU 1 respectively
- Those ACPD Messages (Position of RSU 2 + What time they will reach there + AT will use that time)
- Each eNB 1, 2, and RSU 1 send ACPD Message to RSU 2
- RSU 2 gathering ACPDs and makes a ACPDG which consists of group of authenticated ATs by AT's effective time
- At ACPDG's "effective time" comes, RSU 2 broadcasts **a ACPDG**

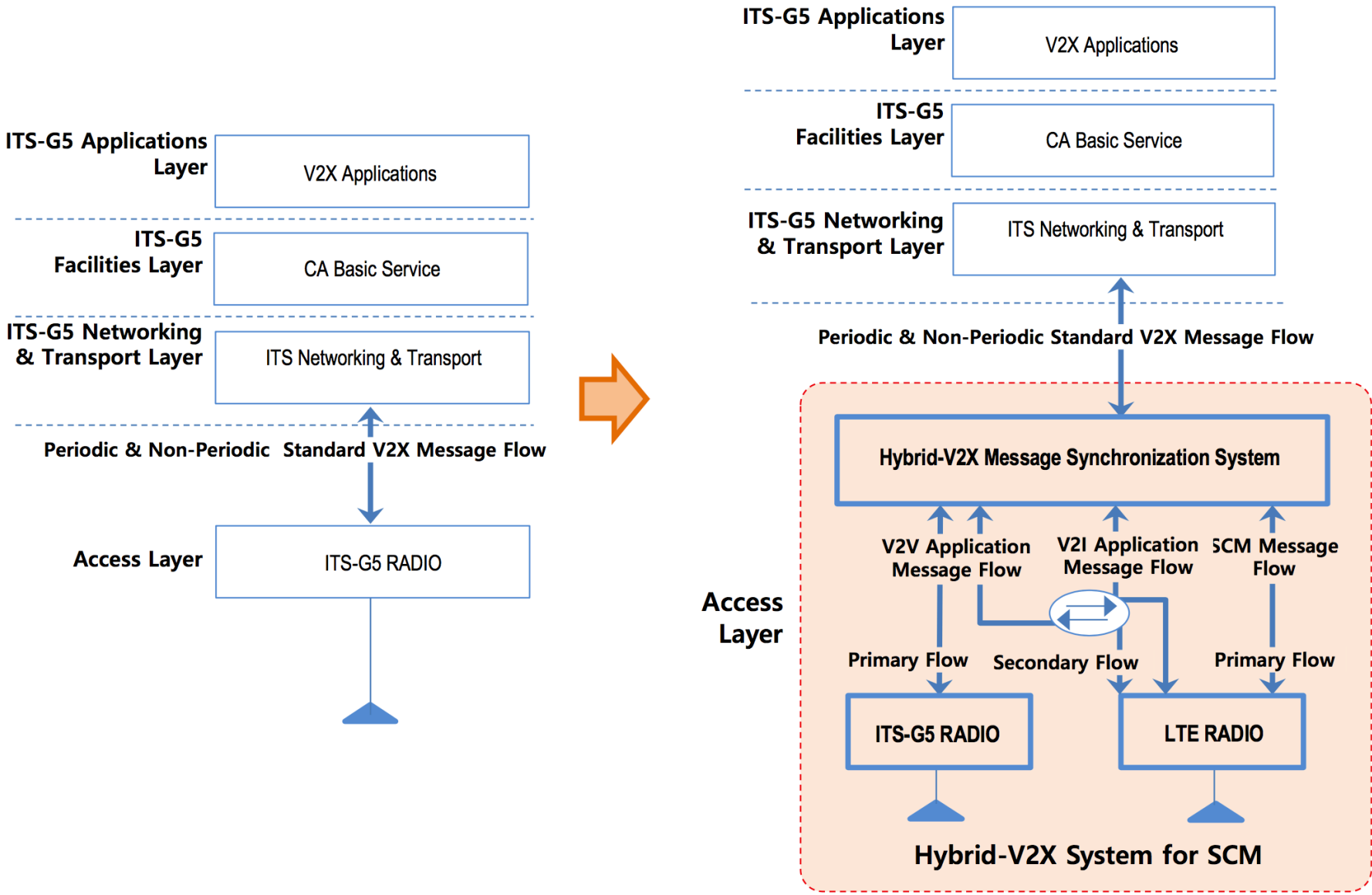


Pros and Cons of ACPD

- **Pros**
  - More suitable for Automated Vehicles
  - Guarantees low latency
  - Decrease channel capacity(by using digests instead of full certificate)
  - Efficient overall management

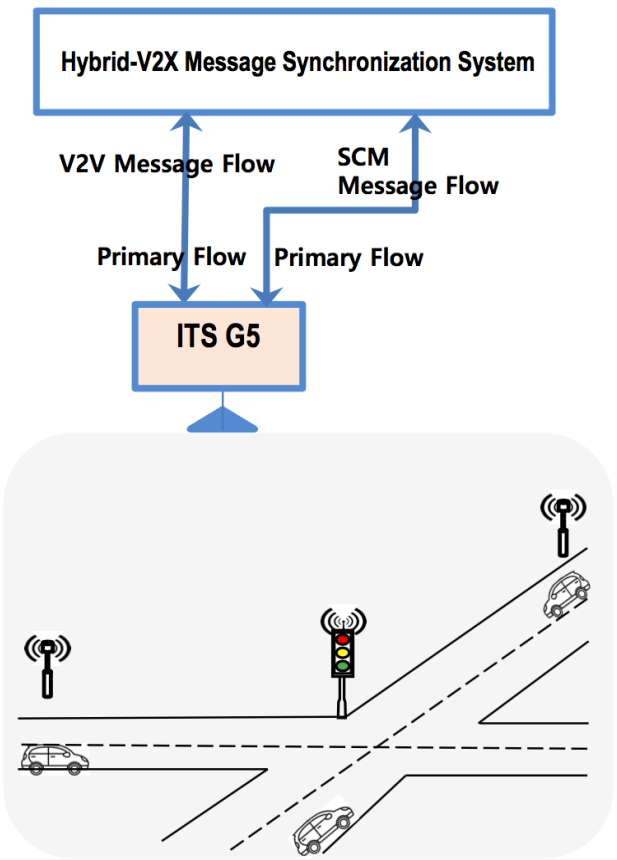
- **Cons**
  - Total number of messages could be increase
  - More storage for Pre-Distributed PCs
  - Implementation complexity more

Hybrid V2X Message Synchronization System

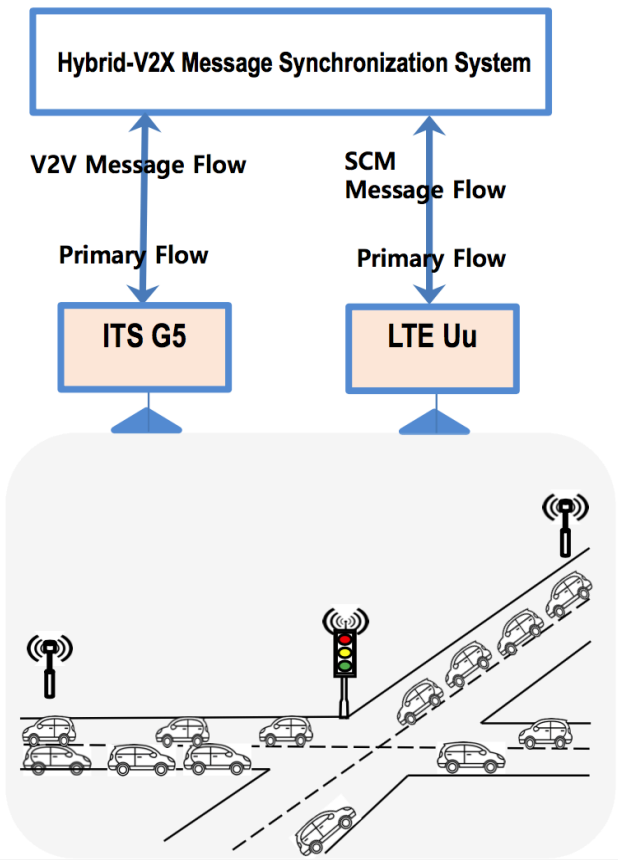


V2V and SCM Message Flow on Hybrid Communication

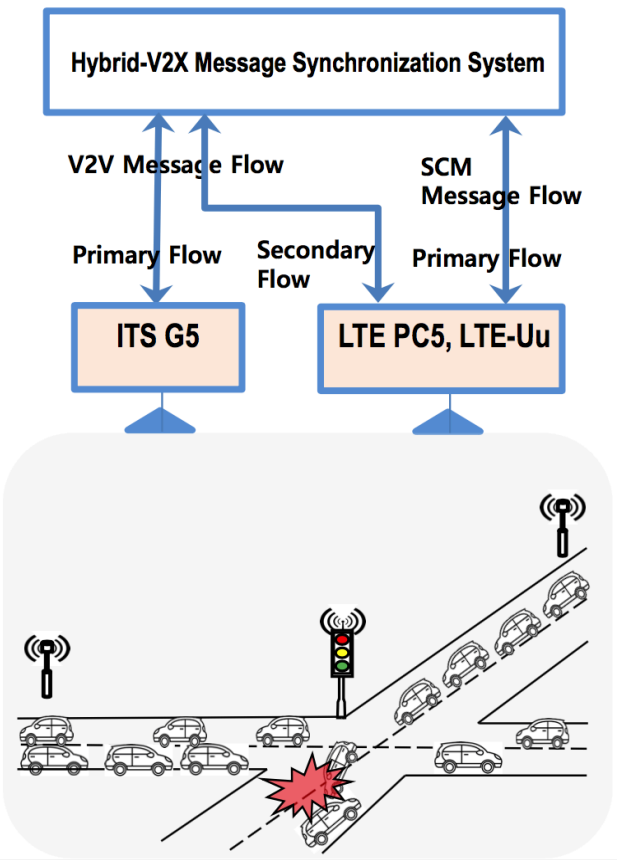
a. Normal Flow for V2V & SCM



b. SCM flow move to LTE-Uu for mitigate Congestion



c. Part of V2V flow move to LTE-PC5 & LTE-Uu for mitigate Congestion



Interface Combination	V2V		SCM/ACPD	
	Normal	Congestion/ Emergency	Normal	Congestion/ Emergency
Primary Interface	ITS-G5	ITS-G5 for more safety/short latency	ITS-G5/IPv6	LTE-Uu
Secondary Interface	LTE-PC5	LTE-PC5 for less safety	LTE-Uu	ITS-G5/IPv6

In Summary

- **V2X for Safety, should be secure as well**

- **Making a secure V2X communication means**
  - All messages should be signed for trust
  - For privacy, all ITS stations need ATs and certificate management
  - All ITS stations need to check validity of AT's signer as often as possible

- **For mitigating the burden**
  - Send predicted effective AT to predicted position for future preparation(ACPD)
  - ACPDG gives effective & verified ATs at once, V2V can keep use the digest.
  - The ACPD automatically activate/deactivate by traffic situation
  - Finally, Security Credential Message(includes ACPD) can be transmitted by using either ITS G5/LTE interface by Hybrid V2X message synchronization system

Merci~

Questions