Cyber Security Study for Automotive Ethernet in Japan Automotive Industry

Japan Automotive Software Platform and Architecture

JASPAR Next Generation High-Speed Network WG

Architecture Team Leader
Mikio KATAOKA
Hitachi Automotive Systems, Ltd.

Architecture Team, Requirement Definition Sub-team Leader
Keisuke Terada
Yazaki Corporation.

7th IEEE-SA Ethernet & IP Automotive Technology Day, San Jose, CA, USA, Nov. 2017

Agenda

1. About JASPAR
   - What's JASPAR
   - Next Generation High-Speed Network WG
   - Activities of WG
2. Status of the Study About In-vehicle Ethernet Security
   - In-vehicle Network Security
   - Study Results
     - JASPAR Supposed Configuration
     - Priority Consideration Items
     - Filtering
     - SSL/TLS
     - VLAN
3. Future Activities
   - Documentation
   - Conclusion

Agenda

1. About JASPAR
   - What's JASPAR
   - Next Generation High-Speed Network WG
   - Activities of WG
2. Status of the Study About In-vehicle Ethernet Security
   - In-vehicle Network Security
   - Study Results
     - JASPAR Supposed Configuration
     - Priority Consideration Items
     - Filtering
     - SSL/TLS
     - VLAN
3. Future Activities
   - Documentation
   - Conclusion

JASPAR: Japan Automotive Software Platform and Architecture

JASPAR was established to pursue increasing development efficiency and ensuring reliability by standardization and common use of electronic control system and in-vehicle network which are advancing and complexing.

■ Mission

- ✓ Improvements in development productivity and significantly contribute to the advancement of the world's technology through standardization activity.
- ✓ Establish of the fair basis for competition of the whole automobile industry.

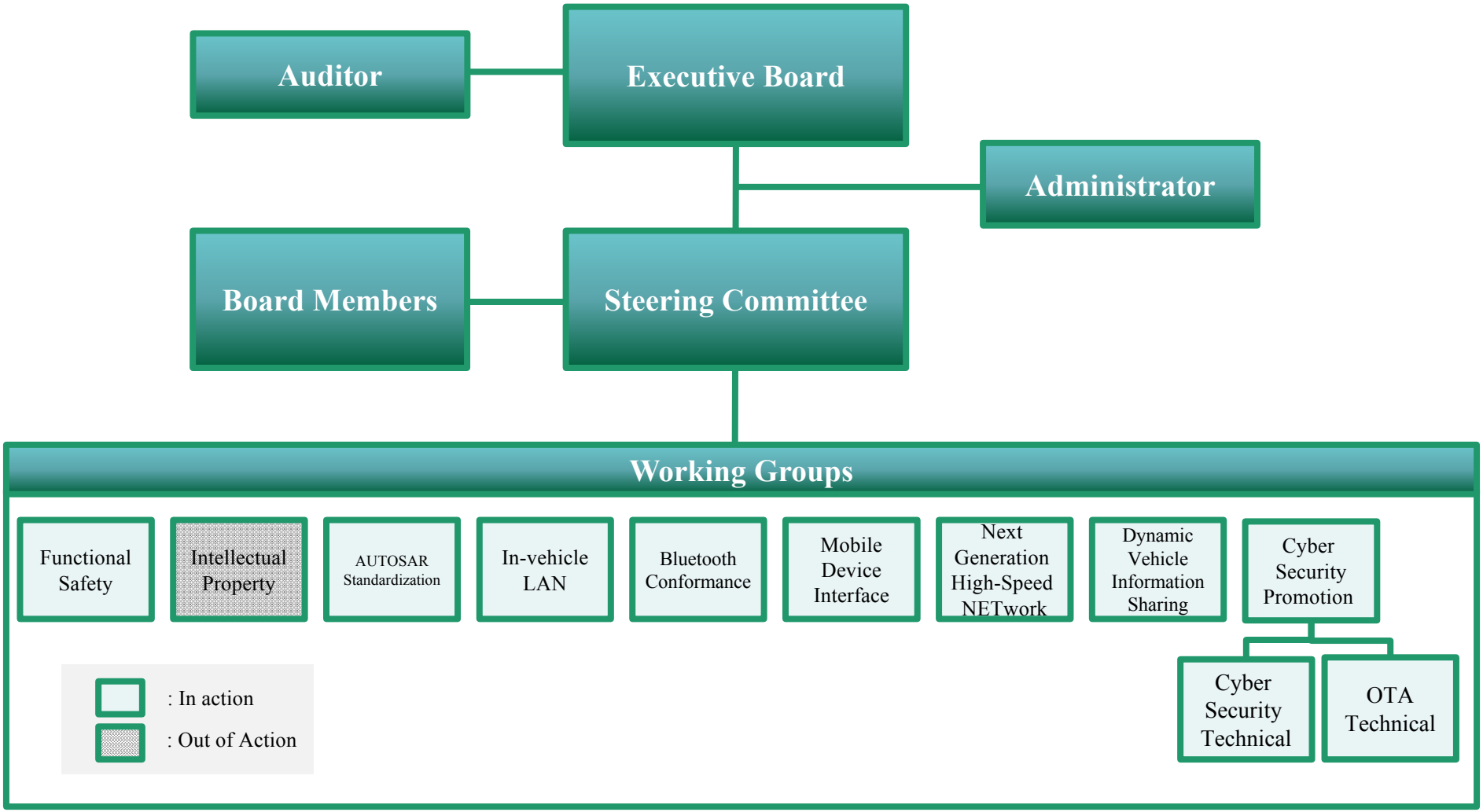
■ Achievements

- ✓ Represent a collective voice of the Japanese companies at the international standardization bodies.
- ✓ Contribute to development of global standards.

1-2. JASPAR members List as of September, 2017

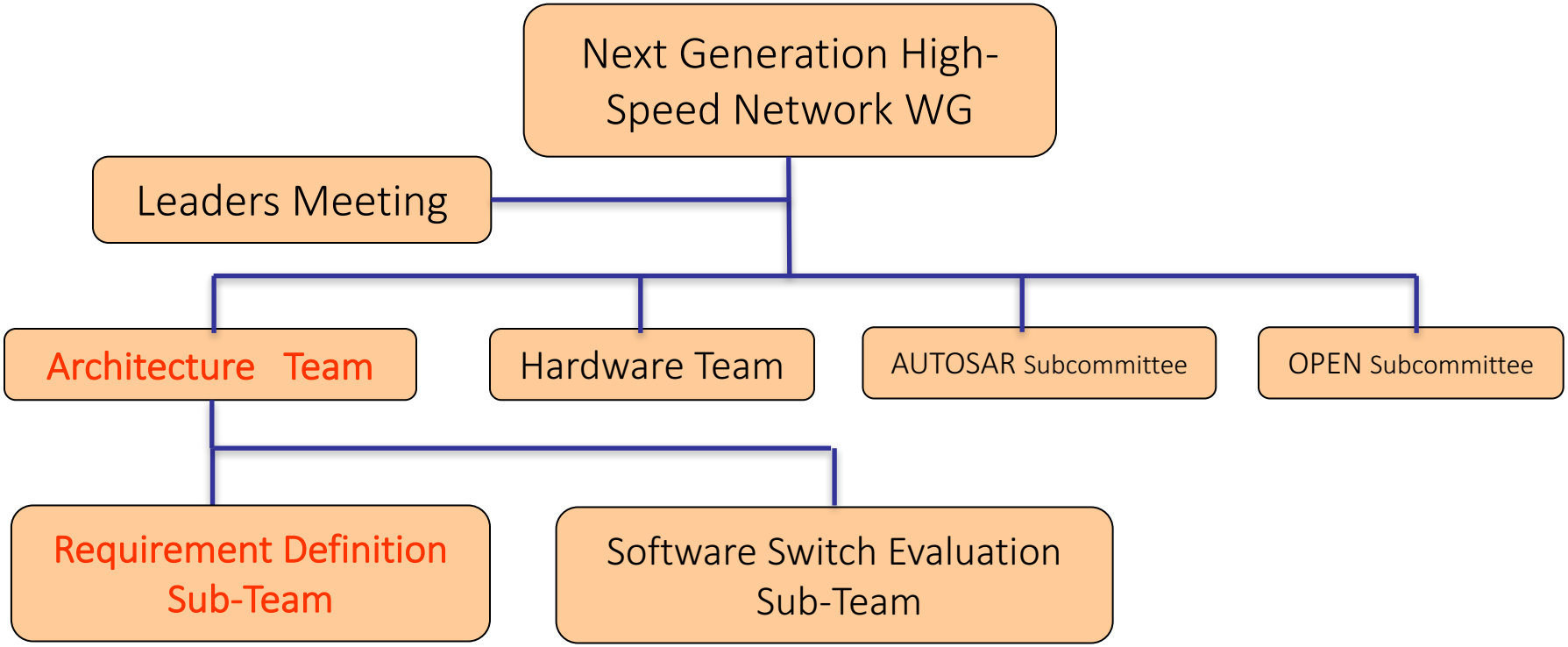
OEM	Tier1	Soft/Tool	Semicon/ Electronics	Others
12	42	73	25	19B
Board member				
HONDA R&D Nissan TOYOTA	DENSO			Toyota Tsusho
Regular member				
ISUZU Mazda SUBARU SUZUKI	ADVICS AISIN AW AISIN SEIKI Akebono Brake Alpine ALPS Autoliv Autoliv Nissin Brake Bosch Calsonic Kansei Clarion Continental Automotive FUJITSU TEN Furukawa Electric Hitachi AMS JATCO JTEKT Keihin Mitsubishi Electric Nidec Elesys NIPPON SEIKI NSK Panasonic PIONEER Ricoh SHOWA Sumitomo Electric TOKAI RIKA Toyoda Gosei TOYOTA INDUSTRIES YAZAKI	ADC APRESIA APTJ ATS AUBASS Cadence CATS Change Vision eSOL ETAS FFRI FTL FUJI SOFT FUJITSU FUJITSU BSC Hitachi ICS IBM Japan KPIT Mentor Graphics micware NEC Nihon Synopsys OMRON OTSL SCSK STABILITY Sunny Giken Toshiba Information Systems TOYO Trend Micro Vector Japan WITZ	Harman International HRS Infineon MegaChips Microchip MJKK Murata NXP Semiconductors Renesas TDK TOSHIBA Tyco Electronics	DNP DTRS KDDI SECOM TOPPAN TOYOTA CRDL
Assciate member				
DAIHATSU Hino HYUNDAI Mitsubishi Motor UD Trucks	Delphi Automotive Systems Fujikura KYB Magna International MITSUBA NGK SPARK PLUG Toyodenso TRANSTRON Valeo Japan Yamaha Motor	A&D A&W Techonology ACCEL JAPAN AIC AISIN COMCRUISE ANRITSU Argus Cyber Security AXE AZAPA BITS Brison Canon ITS Digital Contents DIT dSPACE Eager Eiwa Elektrobit GAIO HI CORP Hitachi High-Tech Ixia LAC Mamezou MITO SOFT NEC Solution Innovators Netagent NTT DATA MSE NTT DATA SBC PCI Solutions Systena Takasaki Kyodo Tata Consultancy TOKYO ELECTRON DEVICE Trillium TTTech Ubiquitous USE Wind River Xilinx Yokogawa	ADI ARM Cypress Innovates HI-LEX Hitachi ULSI Hosiden NTN ROHM Sanden Automotive Components SanDisk Shindengen Thine YOKOWO	Allion Japan Biz3 HAGIWARA Kyoei Sangyo MACNICA NTT DOCOMO OEC RENESAS EASTON Ryoden Ryosan SANSHIN Shinko Shoji

1-3. JASPAR Organization (as of September 2017)



1-4. Next Generation High-Speed Network WG

- Define in-vehicle requirements for the next-generation high-speed network technology.
- Study certification/authentication mechanisms to ensure conformance and interoperability, as required.
- Keep close cooperation with associated domestic/international organizations and companies to accomplish stated goals.



Agenda

1. About JASPAR
   - What's JASPAR
   - Next Generation High-Speed Network WG
   - Activities of WG
2. Status of Study About In-vehicle Ethernet Security
   - In-vehicle Network Security
   - Study Result
     - JASPAR Supposed Configuration
     - Priority Consideration Items
     - Filtering
     - SSL/TLS
     - VLAN
3. Future Activities
   - Documentation
   - Conclusion

2-1-1. Case of the Car Hacking

Hacker trends

Hacking level for cars has increased year by year

FCA recall 1.4 million units

<Target>
Uconnect implemented car.
<Attack>
Control the display, steering and transmission.
(Accidents caused by a remote attack has not occurred.)

'13
Hacking in the car

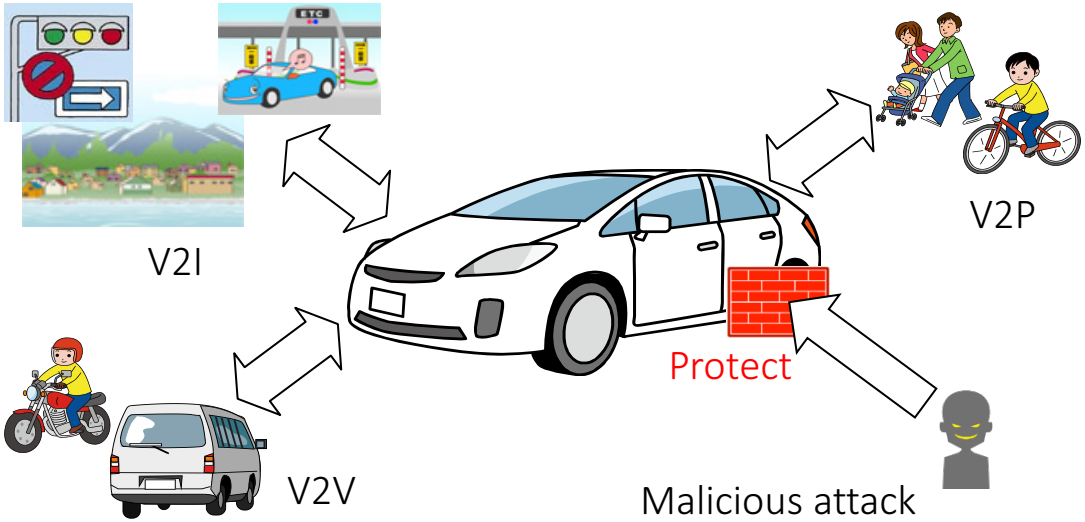
'15
Hacking from remote
(At low speed)

<Target>
FCA Jeep
<Attack>
Send the maintenance command from the diagnosis connector.
Impersonated a regular ECU and control the steering.

'16
Control the car using maintenance mode
(When driving)

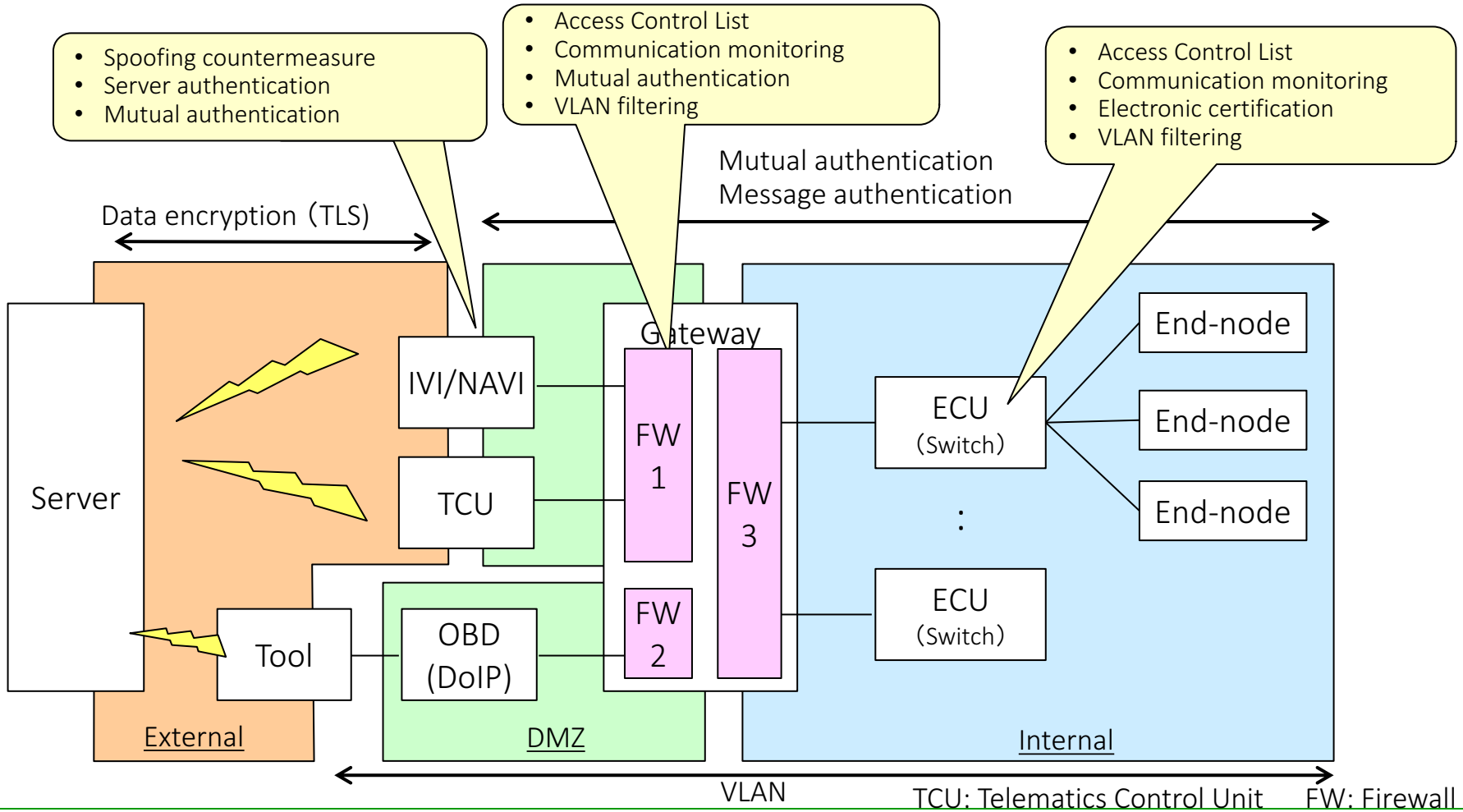
- There are the important issues that we discuss the security measures against cyber attacks.

Also in the Next Generation High-Speed Network WG,
the in-vehicle Ethernet security has been studied from 2015.



2-2-1. JASPAR's Presumed Security Configuration

- The gateway separates outside and inside of vehicle as a attack surface and filters illegal data for intrusion prevention.
- Data communicated with outside of vehicle should be encrypted.
- Message authentication code is adapted for communication data of in-vehicle.



2-2-2. Ethernet Security Technologies

- Enumerate the security technologies related the Ethernet.

Category	Applied layer			Target
	L2	L3	L4 or above	
Filter	Port based VLAN			Input Port
	Tagged VLAN			VLAN Tag
	Private VLAN			Input Port
		Sub network based VLAN		IP Address
	MAC filtering Port security IEEE802.1X MAC Authentication bypass			Mac Address
	Static MAC Table			MAC Address
	Dynamic ARP Inspection			ARP
		IP Source Guard		IP Address
		IP filtering		IP Address
		VLAN ACL		VLAN ID
		NAT(Network Address Translation)		IP Address
		NAPT(Network Address Port Translation)		IP Address＋PortNo.
		DDoS Open Threat Signaling (dots)		Traffic
			OCSP (Online Certificate Status Protocol)	Certification
Intrusion Detection			DPI(IPS/IDS) DPI：Deep Packet Inspection IPS: Intrusion Prevention System IDS:Intrusion Detection System)	payload
			WAF(Web Application Firewall)	http/https
			MAC(Message Authentication Code)	Payload
Cipher	MACsec			Ethernet Frame
		IPSec		IP
			DTLS	UDP/IP
			SSL/TLS	TCP/IP
Authentication			Kerberos Authentication	ID/PASSWORD
			RADIUS (Remote Authentication Dial In User Service)	Identification Information (ID/PASSWORD, Cerfication)

2-2-3. Priority Consideration Items

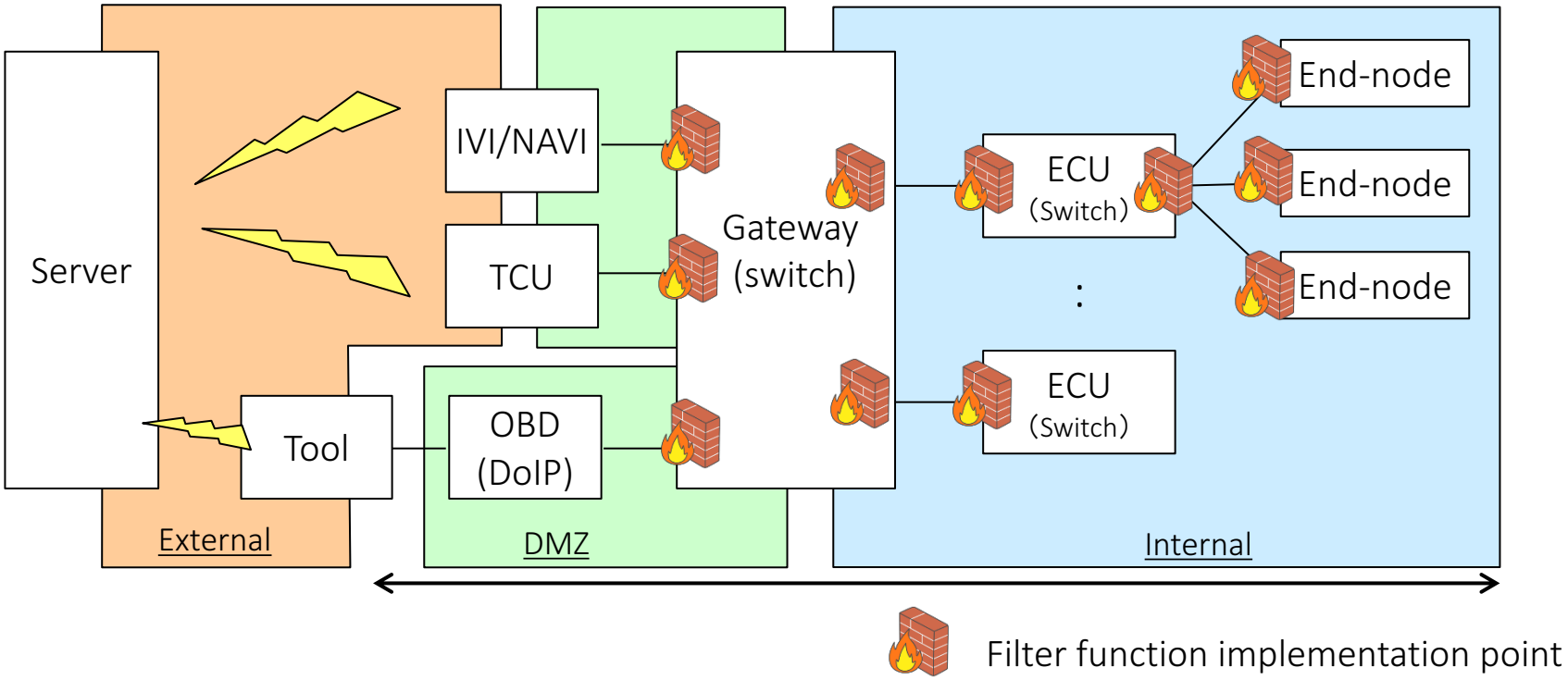
- Priority consideration items are selected for in-vehicle Ethernet network.
  - Decided by the interests of participating companies.
- The following 3 items are selected.
  - VLAN, Filtering, SSL/TLS.

Category	Discussion items
VLAN	•Usage of the VLAN as the network configuration. •Routing using the VLAN. (consider domains)
Filtering	•Scope of filter application as the in-vehicle systems. •Performance of the automotive microcomputer / switch.
Message authentication	•This category is discussed by other WG in JASPAR. So, exclude from discuss point in this WG.
SSL/TLS	•Investigate the specification and the compatibility with the in-vehicle systems. •Performance applied to automotive microcomputer.
DPI	•Investigate the technologies. (what kind of attack can be detected)
MACSec, IPSec	•Feasibility based on required processing capacity Performance in software / hardware.

VLAN: Virtual LAN SSL: Secure Socket Layer TLS: Transport Layer Security
DPI: Deep Packet Inspection

2-3-1. Implementation Point of Filtering

- We discussed the implementation points of filtering.
  As a result, we presume the following points as implementation points.
- By matching between the filtering function set for each point and the received packet, it is selected whether the packet is passed or discarded



2-3-2. Security Technologies Applied to the Filtering

- Select the security technologies as a prerequisite to discuss the filtering function.

  Scope : Standardized or discussing technologies created by

  IEEE, IETF, etc.

Security technologies
Port-based VLAN
Tagged VLAN
Private VLAN
Sub network based VLAN
MAC filtering, Port security, IEEE802.1X, MAC authentication bypass
Static MAC Table
Dynamic ARP Inspection
IP Source Guard
IP filtering
VLAN ACL
NAT(Network Address Translation)
NAPT(Network Address Port Translation)
DDoS Open Threat Signaling (dots)
OCSP (Online Certificate Status Protocol)

2-3-3. Filtering Fields and Applied to In-vehicle Network

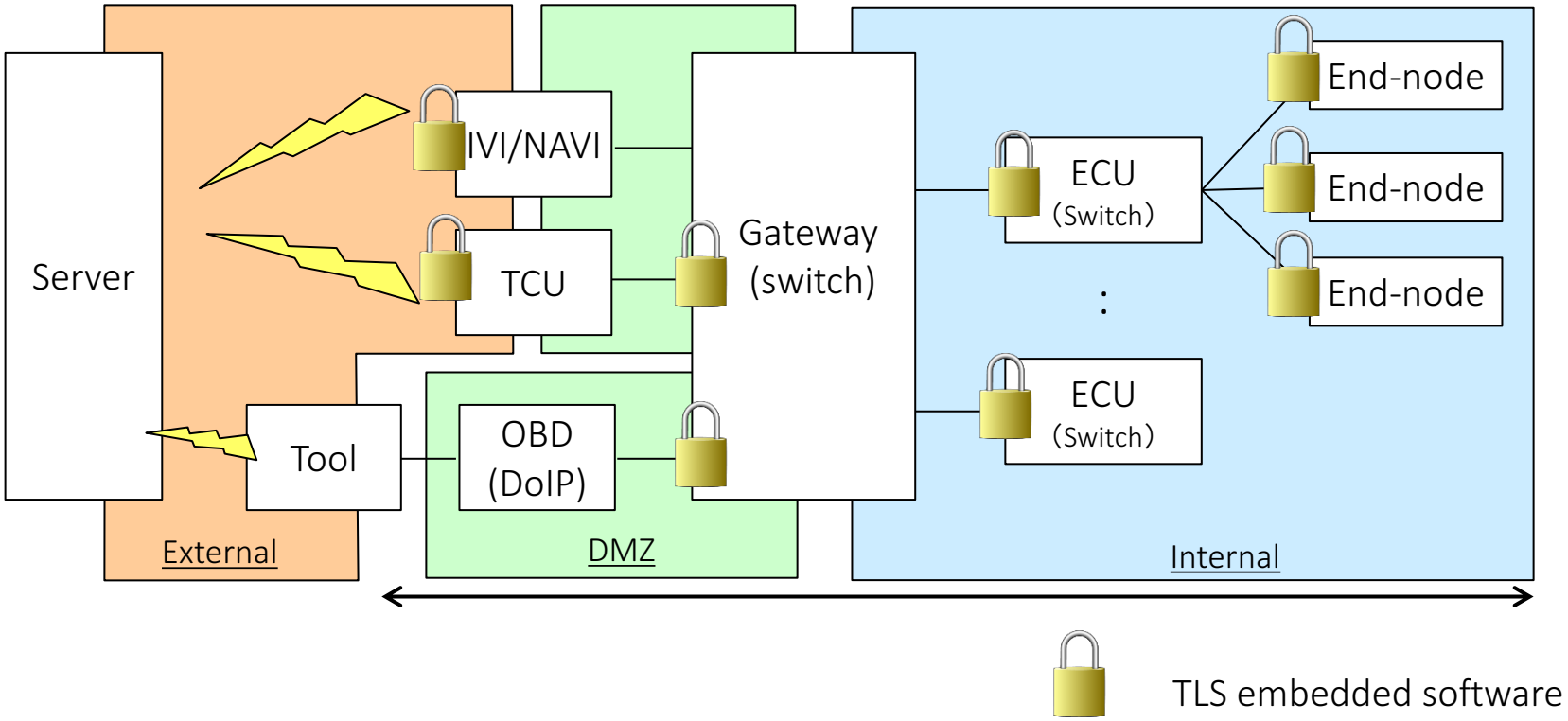
- Enumerate filtering items for each OSI layers.
  - Implementation function.
  - Applied to in-vehicle network.
  - With or without hardware support.

Enumerated filtering items

OSI layers	Filtering items	Overview	Security technologies	Applied to in-vehicle network	Hardware supported
L2	VLAN number	VLAN number	Port-based VLAN	○	○
			Private VLAN		×
	VID(VLAN Identifier)	VLAN identifier	Tagged VLAN	○	○
	Source MAC address	Source MAC address	MAC filtering, Port security, MAC authentication bypass	○	○
			Static MAC Table		○
			Dynamic ARP Inspection		×
	ID, password, Digital certificate	ID, password, Digital certificate	IEEE802.1X	×	×
L3	Protocol number	Type of network protocol in the transport layer	IP filtering	○	×
			VLAN ACL		
	Source IP address	Source IP address	Sub network based VLAN	○	×
			Dynamic ARP Inspection		
			IP filtering		
			VLAN ACL		
			NAT(Network Address Translation)		
			NAPT(Network Address Port Translation)		
	Destination IP address	Destination IP address	IP filtering	○	×
			VLAN ACL		
			NAT(Network Address Translation)		
			NAPT(Network Address Port Translation)		
L4	Source port number	Source port number	IP filtering	○	×
			VLAN ACL		
			NAPT (Network Address Port Translation)		
	Destination port number	Destination port number	Same as above	○	×
I/F	Source port number	Physical port	Private VLAN	○	×
	Destination port number	Physical port	Same as above	○	×

2-4-1. Implementation Point of TLS

- We discussed the implementation point of TLS.
  As a result, we presume the following points as implementation points.
- Since there is a possibility that the internal ECU may become the end point of TLS, the implementation point of TLS is the entire network including gateway, ECU, and end node.



2-4-2.TLS Function and Technologies Related TLS

- Discuss the TLS function and technology elements.
  - Technology overview and recommendation.

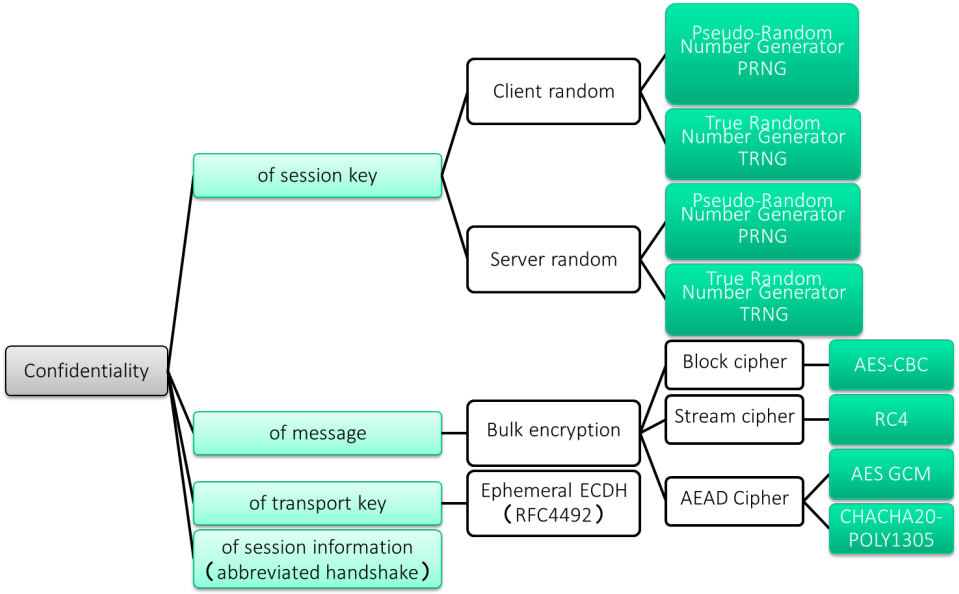
Enumerated technology elements

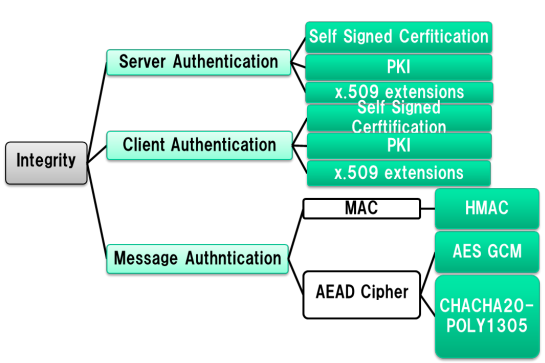
Technology	Overview	Recommendation
PRF	Pseudo-random number generator to generate session keys	○
PRNG	Pseudo-random number generator	○
TRNG	True random number generator	△
RC4	Stream cipher	×
AES-CBC	Block cipher	○
AES-GCM	Authenticated encryption block cipher	○
ChaCha20-Poly1305	Authenticated encryption stream cipher	△
Self-signed certificate, server	Certificate whose signature has been generated by server itself	△
Self-signed certificate, client	Certificate whose signature has been generated by client itself	×
PKI	Public Key Infrastructure for authenticating public keys and their owners	○
X.509	Standard format for certificates	○
SHA	Most commonly used hash standard	○
RSA	One of the public key cryptographic mechanism	○
DHE-RSA	Key exchange done with ephemeral Diffie-Hellman, authentication with RSA signatures	○
ECDHE-ECDSA	Key exchange done with ephemeral Elliptic Curve Diffie-Hellman, authentication with Elliptic Curve DSA signatures	○
ECDHE-RSA	Key exchange done with ephemeral Elliptic Curve Diffie-Hellman, authentication with RSA signatures	△
Server duplication	Multiple TLS servers are provided in order to handle a large number of clients	△
PSK	Session keys are exchanged using pre-shared symmetric keys	○
DHE-PSK	Key exchange done with ephemeral Diffie-Hellman, authentication with PSK symmetric keys	△
RSA-PSK	Key exchange done with PSK symmetric keys, authentication with RSA signatures	△
Session resumption	Previous TLS session data is reused across sessions	○

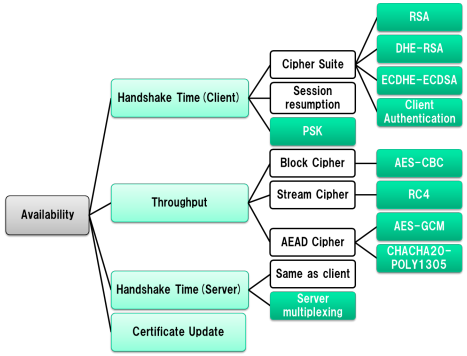
2-4-3.Threat Analysis of TLS Requirements

- Perform the threat analysis by the CIA.
  - Consider Confidentiality / Integrity / Availability and related technical elements.

CIA	TLS Requirements
Confidentiality	Confidentiality of session keys
	Confidentiality of messages
	Transport keys
	Session information
Integrity	Server authentication
	Client authentication
	Message authentication
Availability	Connection times (Server)
	Throughput
	Connection times (Client)
	Certificate renewal

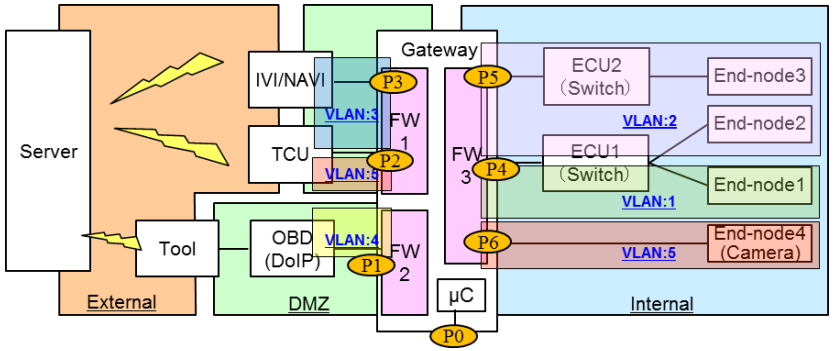






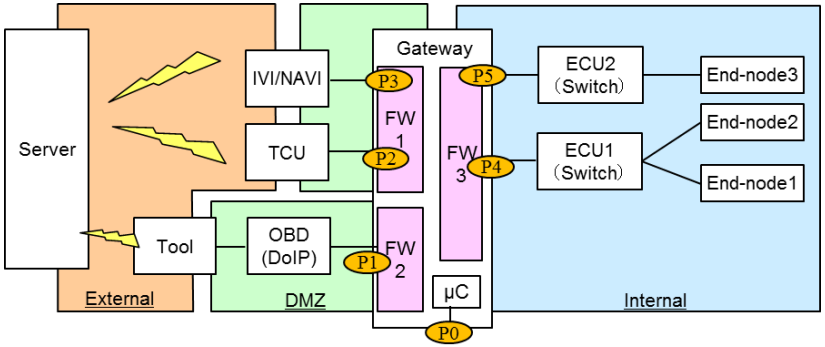
2-5-1. Example of VLAN Configuration

- Discussion of VLAN configuration based on JASPAR network configuration.
  => Classified into two types.
  - VLAN configurations by domain.
    Assign VLAN ID for each network domain.
  - VLAN configurations by application.
    Assign VLAN ID for each application.



Ports	ECU	VLAN Membership				
		1	2	3	4	5
0	μC (Gateway)	x	x	x	x	
1	Tool				x	
2	TCU			x		
3	IVI/NAVI			x		x
4	ECU1	x				
5	ECU2		x			
6	Camera					x

VLAN configurations by domain



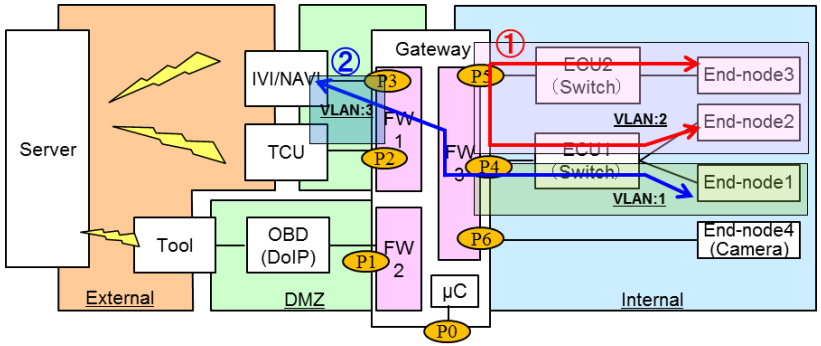
VLAN	Application
10	DoIP(Before auth.)
10	DoIP(After auth.)
20	xxxx1
2x	xxxx2
30	xxxx3
3x	xxxx4

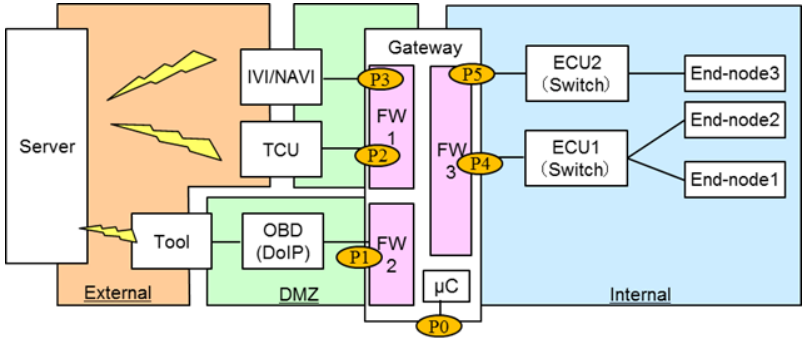
Ports	ECU	VLAN Membership					
		10(B)	10(A)	20	2x	30	3x
0	μC(Gateway)	x	x		x		
1	Tool	x	x				
2	TCU			x	x		
3	IVI/NAVI			x	x		x
4	ECU1		x			x	x
5	ECU2		x		x	x	x

VLAN configurations by application

2-5-2. Example of Firewall Application

- In case of applying a firewall to VLAN configurations.
  => Configure the Firewall to forward packets only to the required ports.





1. Communication within VLAN: End-node 3 ⇔ End-node 2
   Internal(between ECU1 and ECU2)allows filtering to pass.

2. Communication between VLANs:
   IVI/NAVI(VLAN 3) ⇔ End-node1(VLAN 1)
   It is preferable to filter by MAC address, IP address, port number at FW 1 and FW 3 of Gateway.

VLAN	Application
10	FW2 internal comm. (DoIP, before auth.)
10	FW2 internal comm. (DoIP, after auth.)
20	FW1 internal comm. (SOME/IP)
2x	FW1 external comm. (application 1)
30	FW3 internal comm. (IP Video)
3x	FW external comm. (application 2)

Ports	ECU	VLAN Membership					
		10(B)	10(A)	20	2x	30	3x
0	μC(Gateway)	x	x		x		
1	Tool	x	x				
2	TCU			x	x		
3	IVI/NAVI			x	x		x
4	ECU1		x			x	x
5	ECU2		x		x	x	x

VLAN ID 10: Port based VALN
Others: Tagged VLAN

- White list method
  Check the VLAN ID and the L2, L3, L4 headers permitted for each input (physical) port, only transfer the permitted packets

Example of the firewall
in case of VLAN configurations by domain

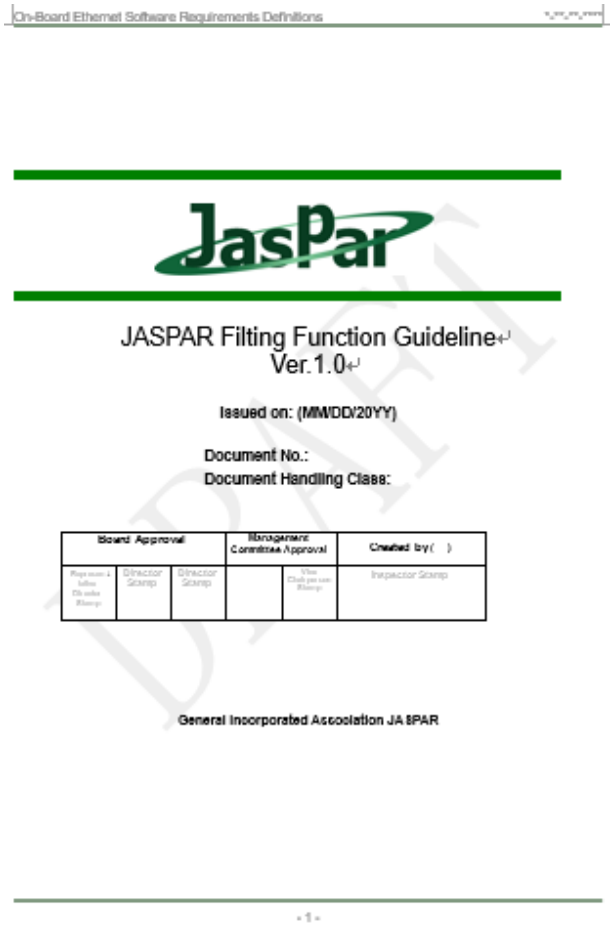
Example of the firewall
in case of VLAN configurations by application

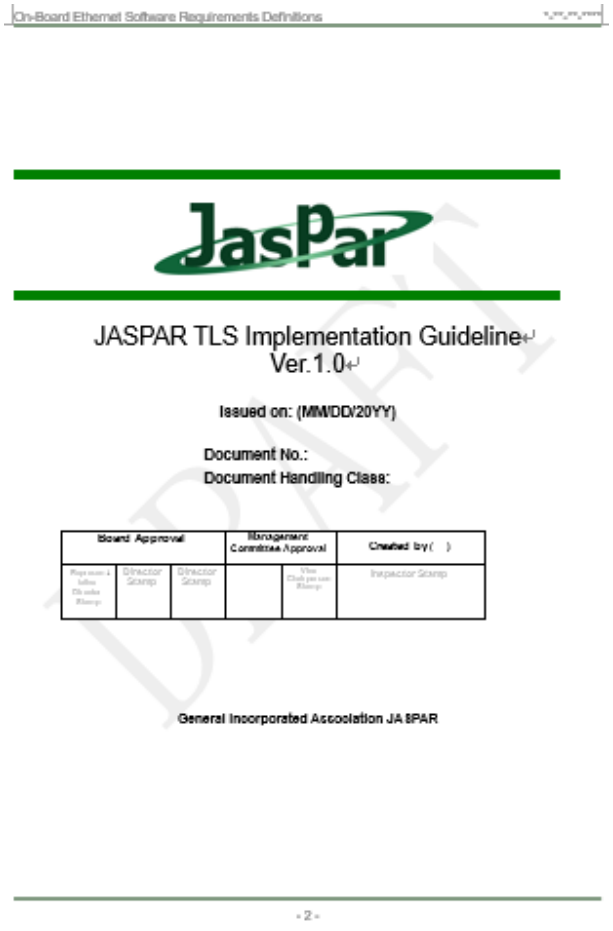
Agenda

1. About JASPAR
   - What's JASPAR
   - Next Generation High-Speed Network WG
   - Activities of WG
2. Status of the Study About In-vehicle Ethernet Security
   - In-vehicle Network Security
   - Study Results
     - JASPAR Supposed Configuration
     - Priority Consideration Items
     - Filtering
     - SSL/TLS
     - VLAN
3. Future Activities
   - Documentation
   - Conclusion

3-1.Documentation

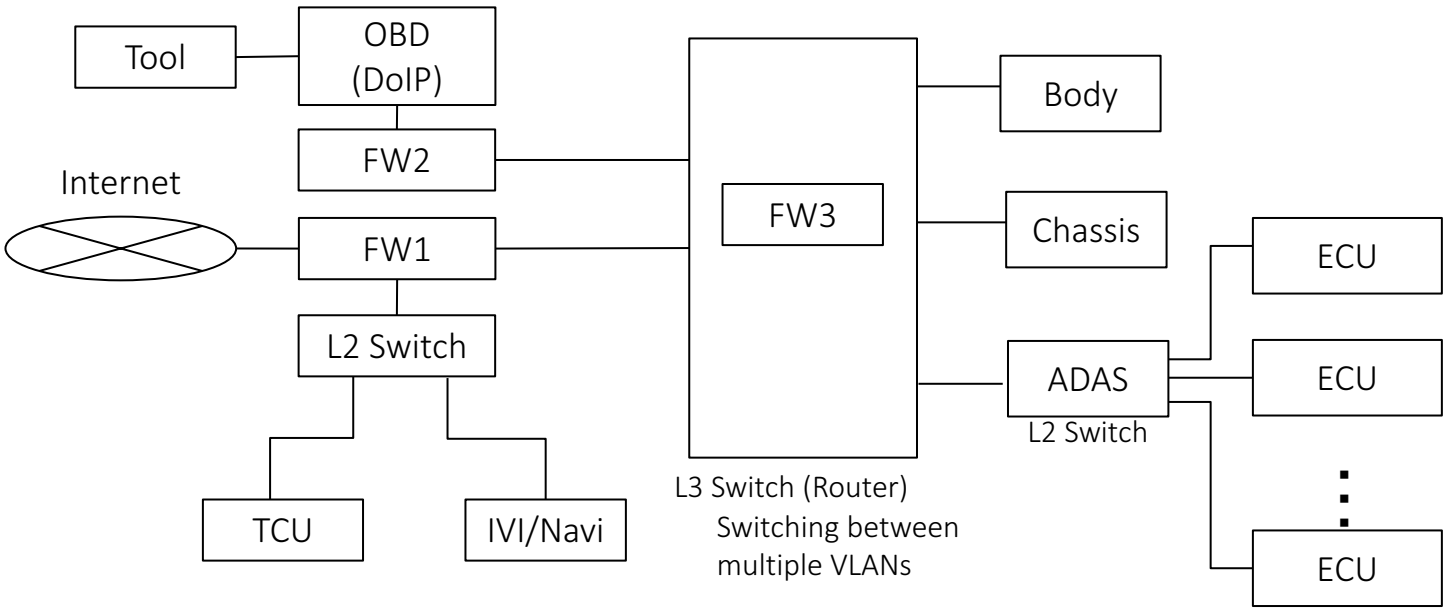
- These results are described for JASPAR guidelines. (within 2017)
  - JASPAR members can obtain these documents.





3-2. Future Activities

- We are discussing the security technology verification of in-vehicle. By comparing ICT(Information Communication Technology) security and in-vehicle security, clarifies different factors.



Configuration example in ICT

- Study of TSN requirements
  Started by investigating specifications,
  under consideration of application examples.

3-3.Conclusion

- Discuss the Ethernet security technologies applied to in-vehicle network.
  - Enumerate the Ethernet security technologies.
  - Select Filtering, SSL/TLS and VLAN for the priority consideration items.

	Discussed items	Output
Filtering	- Enumerate the filtering items. L2 : VLAN ID, TPID, VID etc. L3 : Protocol number, Control flag (SYN) etc. - Define the implementations of hardware or software.	- Define the requirements of the filtering items.
SSL/TLS	- Discomposed the SSL/TLS technologies into functional elements. Authentication method, Encryption, Connection time and Throughput etc.	- TLS technologies guideline. - Clarify the use case, used technologies.
VLAN	Define the network architecture with VLAN. - VLAN configurations by domain. Network design (including multi-VLAN) - VLAN configurations by application. Network design (DoIP, Image transmission, Map data distribution etc.)	- VLAN design guideline. - VLAN design architecture and required technologies.

Thank you for your attention.