August 2020

Preparing for regulated automotive over-the-air updates

A Guide to WP.29 OTA and ISO/AWI 24089

About SBD Automotive

Management & technology consultants to the automotive industry for over 20 years

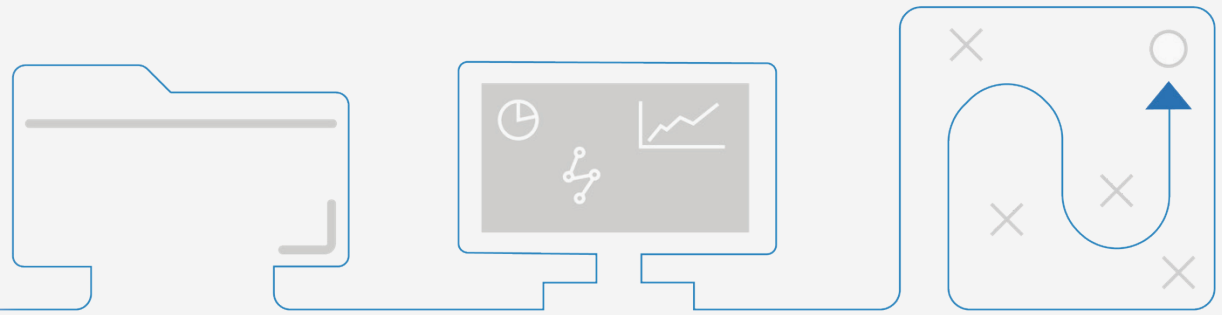
Our expertise:

- Connected
- Autonomous
- Shared Mobility
- EV
- Cybersecurity
- Anti-theft

Our role:

As our industry faces... **Uncertainty** ▶

We provide our clients with... **Data** ▶ **Insight** ▶ **Advice**



Seeing Beyond Data

Turning data into actionable advice

Click to find out more

Research Portfolio

Consulting Services

Contact Us

Defending the defenses…

The proliferation of over the air software update capabilities for automotive OEMs has created massive opportunities for new business models and consumer experiences. It also provides a fundamental weapon in the OEM's arsenal of cybersecurity countermeasures – the ability to remotely patch vulnerabilities is a fundamental need for highly connected and autonomous vehicles.

However...

Software updates systems also represent a juicy target for hackers – privileged access to software update mechanisms is one of the main vectors used to exploit remote systems. Providing a secure over the air update capability with appropriate controls to ensure functional safety is the core intent of the WP.29 remote software update resolution which will guide type approval regulations in many member countries. This insight intends to show the main elements of the resolution, the intent of the associated ISO standardization activity, and recommendations for companies involved in the OTA value chain.

OTA Engineering Team

Jeff Huron
Senior Specialist

Simon Halford
E/E architecture

Paul Sanderson
End-to-end

Alex Oyler
Head of Car IT

Jithesh Joshy
Wireless/SDR

Guillaume Ouellette
Senior Specialist

Masahiro Otsuka
Research

What is WP.29 OTA?

Requirements

- **Specific documentation** is required from OEMs, ECU suppliers, and OTA vendors to achieve compliance
- **Clear business processes** to control the OTA update process and assist in determining current software versions and related auditing requirements
- **New cybersecurity processes** are required throughout the software delivery process, from supplier/vendor to installation in the vehicle
- **Long-term documentation storage requirements** as potential evidence for regulators & auditors

Timing

June 2020 - The final version of WP.29 Software Updates was adopted by the UN.

August/September 2020 – Initial national legislation in Japan expected to be released

November 2020 - First countries with legislation will go into force requiring special permits for software updates which affect a Type

January 2022 – Requirements applied to new types (first countries)

Coverage

Japan (2020) will likely be the first country to adopt the software update type approval regulations

South Korea, United States, European Union, and UK were all active members in the development of the proposal and are likely to adopt similar regulations

Consequences

For OEMs who do not have compliant update systems, **new models will not be type approved for the target market** which applies the proposed guidelines.

For non-compliant updates, OEMs could face **revocation of type approval** for vehicles not in compliance with the guidelines.

If an OEM applies a software update which requires a modified type approval without following the correct process, in Europe, the commission may be able to revoke type approval as well as apply **per-vehicle financial penalties**.

A brief history of software updates in automotive

”Just in time”
2000s

OEMs use remote update technology in plants for “just in time” updates

Tesla Model S
Early 2010s

Tesla becomes first OEM to offer embedded, “full vehicle” updates with Model S platform, also demonstrating flaws with type approval process

Supplier consolidation
Late 2010s

OTA startups are acquired by large service providers & Tier 1s, setting the stage for mainstream OTA supply chain

Tethered updates
Mid-2000s

Some OEMs offer updates to tethered media applications via solutions such as Airbiquity’s Choreo app platform

Mainstream OTA
2015 onwards

Due to high-profile security incidents, OEMs begin implementing OTA technology for connected components

UN WP.29
2020

Type approval guidelines to be updated to certify OEM OTA systems and post-production updates

What is WP.29 and how does it relate to ISO?

In June 2020, the UN adopted three new regulations aimed at supporting the development of connected and automated vehicles. For the first time, OEMs will need to meet binding requirements on cyber security, software updates and SAE Level 3 automated driving systems. This guide will focus on the UN's software update regulation and its impact on OEMs and suppliers. It will also discuss the pending ISO standardization activity which will guide OEM development efforts to achieve compliance with WP.29

UNECE

WP.29 is the UN Working Party responsible for developing new automotive regulations

UN WP.29
SAE L3 Automated Vehicle (ALKS)

Note. The driver remains the back-up to L3 systems

UN WP.29
Cyber Security

ISO/SAE 21434 provides one option for meeting WP.29 Cyber Security.

UN WP.29
Software Updates

Includes OTA & 'wired' updates.

ISO

SAE INTERNATIONAL

ISO 26262
Functional Safety - Road Vehicles

ISO/PAS 21448
Safety of the Intended Functionality of road vehicles

ISO/SAE 21434
Cyber Security

ISO/AWI 24089
Road vehicles software update engineering

SBD Click to open

"WP.29 non-compliance could prevent OEMs from launching new models and even lead to sales of existing models being halted. This represents a significant threat to an OEM's business.

What's involved with WP.29 Software Updates?

WP.29 Software Updates consists of two major tenets that OEMs must comply with: a secure software update management system (SUMS) and a process for modified type approval resulting from software updates which affect any function on the vehicle which is part of the regular type approval process. The SUMS is checked for each vehicle which is submitted for type approval, and the OEMs are obliged to self-regulate the modified type approval process. Furthermore, the SUMS must be re-certified at least every three years.

1. Software Update Management System (SUMS)

For every given model which is type approved, an OEM must independently assess the overall Software Update Management System (SUMS) which manages the transfer, security, installation, and reporting of software updates and relevant metadata in both the vehicle and the cloud.

The SUMS is certified for each unique type-approved model as in-vehicle technology or architecture can change despite a common backend/cloud solution.

OEMs must arrange an audit of its system through a certified technical service. Such service providers would independently verify regulated items such as:

- Process for identifying updates which affect type approval
- Security for delivering updates to vehicles
- Process for notifying users of relevant updates and associated notes
- Safe execution of updates during driving or while parked
- Clear documentation of update dependencies and rollback technical process

The SUMS for a specific model must be re-certified at least every three (3) years; without re-certification, the approval authority may disallow further updates.

2. Modified Type Approval for Software Update

For any given software update to a type approved model, the OEM will be required to manage an internal process whereby the OEM judges whether or not the update affects the functionality of type approved systems.

If the update does not affect the type approved functionality of the vehicle, the OEM may proceed with the update without any specific notification to the approval authority (government) managing the type approval for the model.

If the update **does** affect the type approved functionality of the vehicle, the OEM must contact the approval authority with a prescribed set of documentation to specifically describe the updated components, functional changes, quality assurance procedures, and verifiable (i.e. hashes) fingerprints of associated software versions.

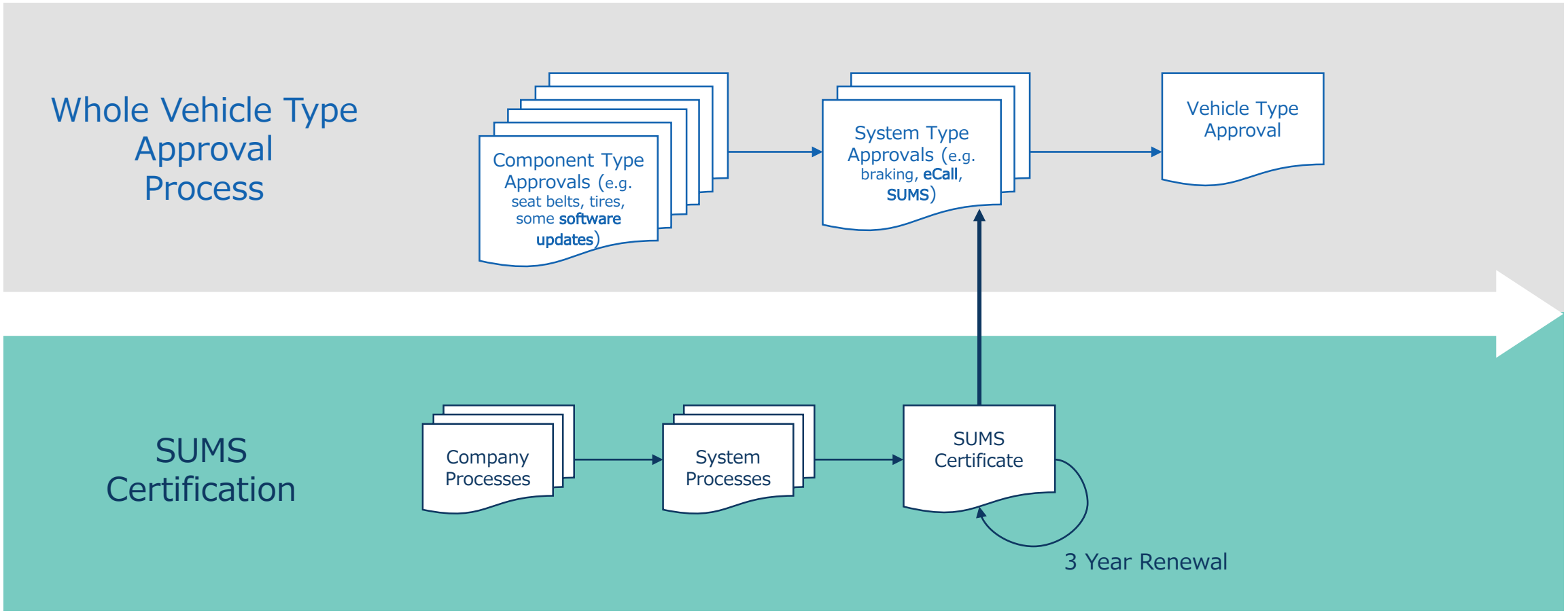
In order to efficiently track type approved software versions, the proposal suggests the usage of **RXSWIN**, or Regulation X Software Identification Number. This version represents the set of software versions installed on all components on the vehicle. The RXSWIN is iterated any time a modified type approval is required, and each RXSWIN version number will have a unique set of software versions associated with it.

Additional notes

- WP.29 Software Updates defines what OEMs need to do, but it does not define how. It is likely that ISO 24089 will act as a functional requirements document for OEMs developing a SUMS and associated process; however, due to the delayed development of the ISO, OEMs will need to ensure preparedness for the regulation in absence of the ISO standard
- The UN is currently developing an 'Interpretation document' that will help OEMs and suppliers to better-understand the WP.29 requirements

How SUMS & vehicle type approval processes correlate

Whole Vehicle Type Approval of an OTA-capable vehicle will require evidence of SUMS conformance. Once the vehicle is type-approved, updates can be sent to vehicles. If those updates impact type-approved systems, those updates will also require approval. If SUMS is not renewed, there may be problems with receiving approval for specific software updates, and conformance checks could be made by approval authorities.



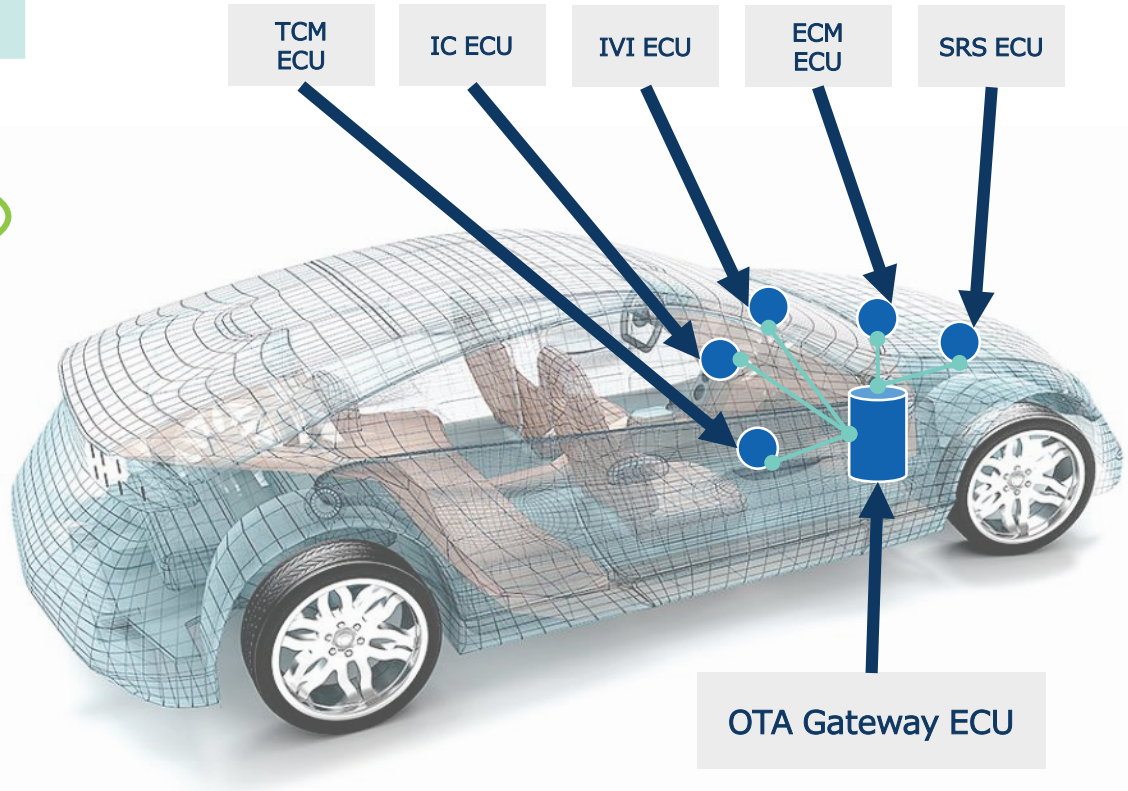
What is “RxSWIN”?

- RxSWIN, short for *Regulation X Software Identification Number*, is the construct defined within WP.29’s OTA standard for versioning whole-vehicle software levels as it relates to specific type approvals and supplementary type approvals
- A vehicle’s RxSWIN must be technically accessible via a trusted, automated method such as OBD-II, or, at minimum, on a compliant OEM backend (via SUMS)
- RxSWIN is a new technical requirement for OEMs, and a scheme must be devised to not only version vehicle software levels procedurally, but also to implement a record of the RxSWIN within both the backend and potentially the vehicle

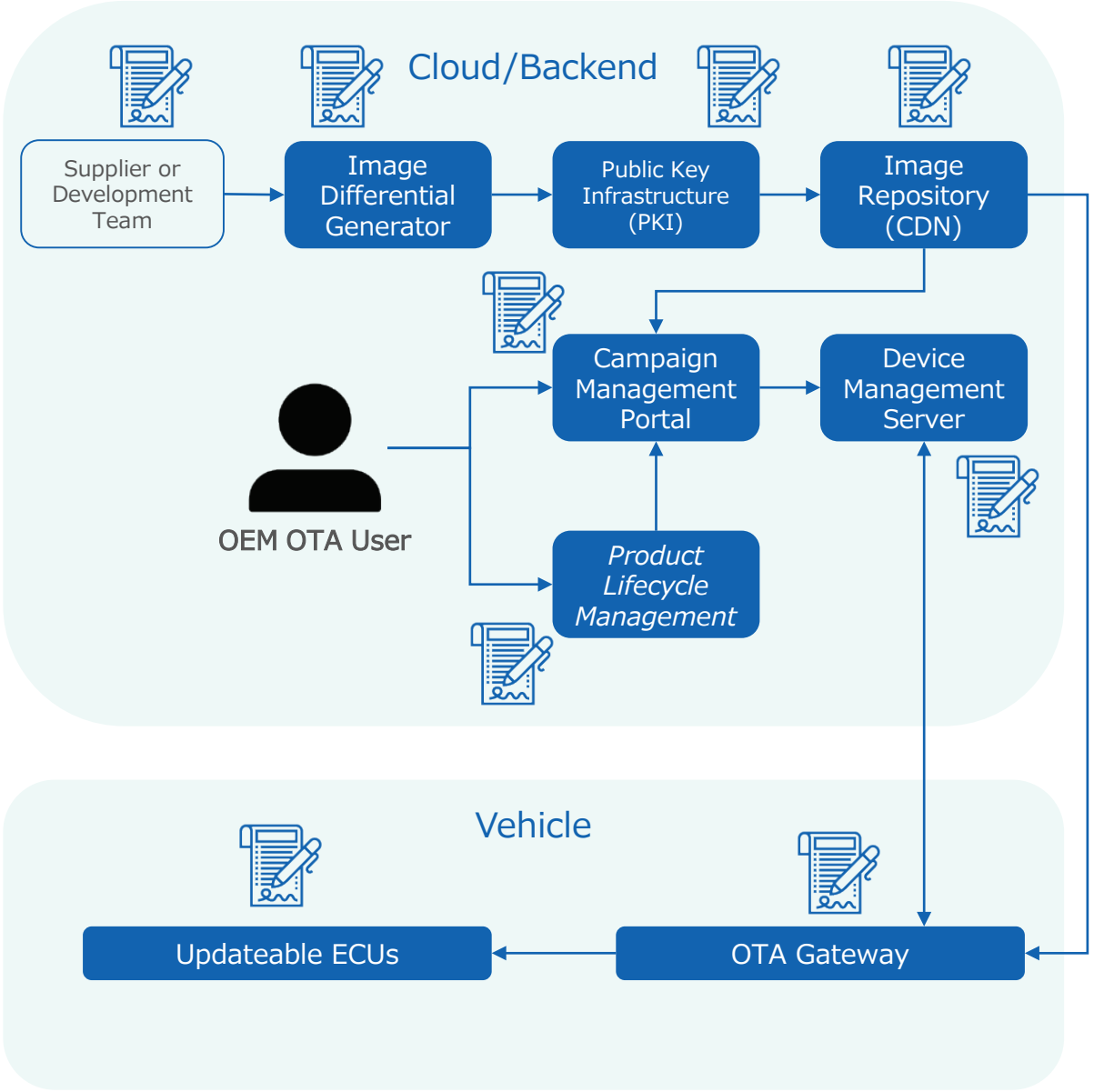
RXSWIN iterated due to new ADAS function which required type approval

RXSWIN not changed as no type approval necessary for IVI app

RXSWIN Level:	R5SWIN 0001	R5SWIN 0002	R5SWIN 0002
Software Change:	Baseline	ADAS function added	IVI app added
OTA Gateway Software Version	1.0	1.0	1.0
TCM ECU Software Version	1.0	1.1	1.1
IC ECU Software Version	1.0	1.1	1.1
IVI ECU Software Version	1.0	1.1	1.2
ECM ECU Software Version	1.0	1.1	1.1
SRS ECU Software Version	1.0	1.0	1.0



What platform components are generally included in a SUMS?



Major components within OTA platforms include:

- **Image Differential Generator** – compresses software updates to only contain the changes between existing software and new software to reduce file sizes
- **Public Key Infrastructure** – suite of cybersecurity services responsible for managing shared secrets, certificates, and other cryptographic enablers required to authenticate software updates and endpoints
- **Image Repository** – platform component responsible for storing software update files securely and distributing to vehicles, often times through a content delivery network (CDN)
- **Campaign Management Portal** – web interface used by OEMs to configure update campaigns to vehicles in the field as well as generate reports for ongoing campaigns
- **Device Management Server** – backend component responsible for tracking currently installed software versions, target software versions and campaigns, and sending update commands to vehicles
- **OTA Gateway** – the device the in vehicle responsible for communicating with the OTA backend as well as distributing and/or installing software to components in the vehicle securely
- **Updateable ECUs** – ECUs which are eligible to receive remote software updates which often contain client software which manages differential software updates and associated integrity cybersecurity requirements

For more information on OTA platforms, technical requirements, OEM strategies, and supplier capabilities, please refer to SBD's extensive research in *Automotive Over the Air Updates Ecosystem 2020*

What are the major supply chain requirements for WP.29 OTA?

While almost all OEMs have already introduced some form of OTA updates, very few have done so across a broad swath of their product portfolio. Additionally, most have not deeply considered the organizational impacts of software updates. WP.29 will force OEMs to deeply consider both the organization supporting OTA processes and capabilities as well as the technical requirements for their OTA update technology suppliers.

	OEM	Component & Software Suppliers	OTA Service Providers
Software Update Management System Requirements			
Process	✓ Compliance documentation storage ✓ Target vehicle identification ✓ Type approval impact identification ✓ Documentation for all software updates		✓ Appropriate approval workflows in all supporting software ✓ Tools for OEMs to manage process ✓ Documentation storage facilities
Components	✓ Record of vehicle software versions ✓ Software dependency management		✓ Data warehouse for all update recordkeeping
Security	✓ Verifiable data integrity ✓ Secure update process & storage		✓ Secure storage of data and update files (if stored with provider) ✓ Security logs for web portal access ✓ Hashing algorithms for verifiable data
Auditing	✓ Campaign recordkeeping ✓ RXSWIN historical register for each vehicle		✓ Cold storage for all update interactions with all vehicles ✓ Hot storage for current vehicle software version information
Modified Type Approval Requirements			
Process	✓ Identification of impact to type approved systems for any software update	✓ Release notes for major software updates to OEM	✓ Compliance workflow on management portals
RXSWIN	✓ Appropriate RXSWIN versioning when type approved system is modified	✓ Consistent software versioning	✓ Fields and data structure to manage RXSWIN versioning
Quality Assurance	✓ Rollback procedures ✓ Driver safety during update process	✓ Security testing ✓ Integration testing	✓ Detailed reporting for status of update campaign
Customer Notification	✓ Update status notifications ✓ Update release notes/scope of changes	✓ Required time to update component (w/ OEM)	✓ Tracking of customer notifications ✓ Notification tools

Quick start checklist for OEMs and suppliers

Time is short for getting WP.29-ready for software updates. While the OEMs who have been managing software updates for years require only minor changes to support WP.29's requirements, many who are just now implementing software updates have neither the organization nor the platform to support regulatory requirements. Here are a few immediate actions for those OEMs looking to move quickly, echoing our recommendations for compliance with WP.29 cyber security:

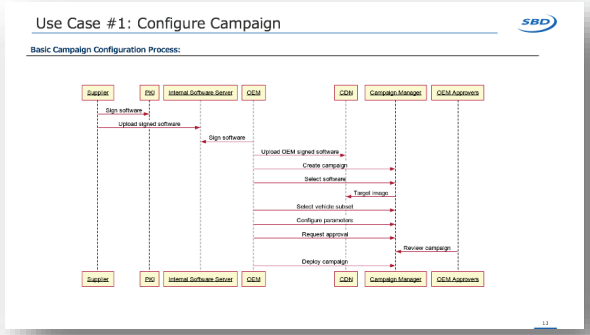
Steps	OEMs	OTA Service Providers
1 Raise awareness	❑ Educate all impacted organizations about WP.29 ❑ Establish WP.29 "tiger team" ❑ Share information with impacted suppliers	❑ Share main technical findings with engineering teams ❑ Reach-out proactively to your customers ❑ Create supplemental briefing/whitepaper to document WP.29 readiness to customers
2 Perform a gap analysis	❑ Document existing OTA process & capabilities ❑ Compare existing OTA capabilities with required capabilities ❑ Prepare new requirements to suppliers for compliance	❑ Benchmark your existing processes ❑ Develop new features & functions in accordance with requirements ❑ Update your contracts and service agreements
3 Start a POC	❑ Use a real software update to test the new process ❑ Limit the scope of POC to manageable size ❑ Perform mock compliance test for SUMS with 3rd party	❑ Perform audit "fire drills" to ensure all data can be collected ❑ Audit platform capability with 3rd party ❑ Develop tools to share best practice

SBD's holistic OTA & connected car support

SBD's heritage is steeped in the underpinnings of remote software updates and cybersecurity. Our global team of experts bring to bear an unrivalled mix of expertise in product planning, technical design, quality assurance, and cybersecurity know-how for connected, autonomous cars.

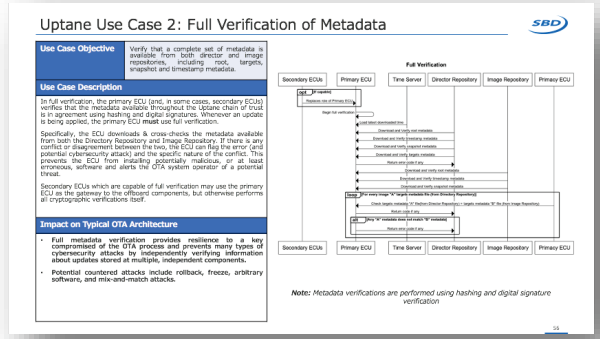
Design

- OTA platform requirements
- OTA components and protocols
- Integration, API, and cybersecurity design
- Supplier sourcing & contracts
- Business process design for compliance activities



Test

- Mock compliance testing for WP.29 SUMS
- Update "fire drills" for testing business processes
- Testing of user experience/in-vehicle update process
- Cybersecurity design & penetration testing



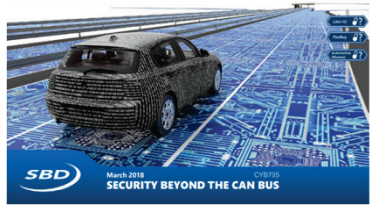
Strategy

- Competitor benchmarking & market trends
- OTA trends by OEM
- OTA product & vendor market analysis
- Market-specific regulatory and competitive assessments

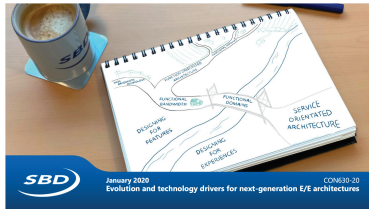
Reports

Automotive Over the Air Updates Ecosystem (633)

Connected Services Guide (526)



Security Beyond the CAN Bus (705)



E/E Architectures (630)

Infotainment OS & Ecosystem (629)

Contact information

North America
Hailey Lueck
haileylueck@sbdautomotive.com
+1 734 619 7969

Germany + North/Central/East EU
Andrea Sroczynski
andreasroczynski@sbdautomotive.com
+49 (0) 211 9753153-1

West & South EU
Alessio Ballatore
aballatore@sbdautomotive.com
+44 74 71 03 86 22

China
Victor Zhang
salesChina@sbdautomotive.com
+86 18516653761

Japan
SBD Japan Sales Team
postbox@sbdautomotive.com
+81 52 253 6201

www.sbdautomotive.com