SYNOPSYS®

WHITE PAPER

Enabling Centralized ADAS Domain Controller SoCs with Automotive IP

Authors

Ron DiGiuseppe,
Automotive IP Segment Manager

Introduction

According to the National Highway Traffic Safety Administration (NHTSA), 94 percent of all automotive accidents are caused by the driver's poor recognition, poor decision making or poor performance[1]. Automotive OEMs are adding new advanced driver assistance systems (ADAS) to improve safety for functions such as automatic emergency braking, pedestrian detection/avoidance, lane departure warning/correction, traffic sign recognition, surround view, drowsiness monitoring, and other applications, as seen in Figure 1. Driven by consumer desire and government regulations to improve road safety, auto makers are adding multiple advanced ADAS applications to new car models. The SoC for these advanced ADAS applications must be designed per the ISO 26262 functional safety standard.

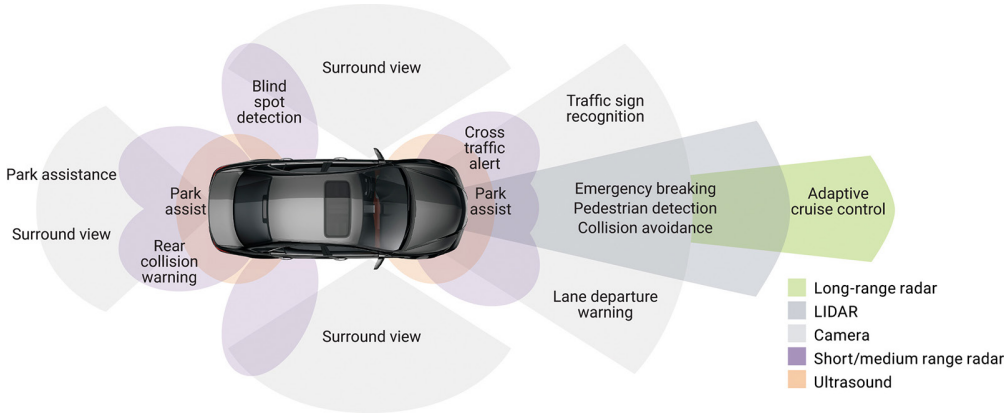


Figure 1: Advanced driver assistance systems improve safety

In today's car, the electronic control units (ECUs) for ADAS applications are distributed throughout the car. However, a centralized architecture is becoming more popular to integrate the ADAS applications into a centralized ADAS domain controller such as Aptiv's (formerly Delphi) multi-domain controller (MDC) module, as seen in Figures 2 and 3. A centralized architecture reduces cost, minimizes development of separate software applications and reduces system complexity. As automakers adopt MDCs with centralized ADAS processors, the required performance and functionality of the ADAS processors increase which requires OEMs, Tier 1 and semiconductor suppliers to develop ADAS SoCs that incorporate the latest interface standards, run multiple vision-based algorithms, and combine image and radar system sensor data.

It is estimated that the existing automotive architecture, using distributed ECUs, will be replaced by a centralized architecture using less than 10 centralized high-performance computers with sensor data supplied by more than 200 sensors[2]. To implement the advanced protocols required to integrate the complex functionality and meet high-performance operations, next generation of ADAS processors must use leading edge SoC design and process technologies compared to current automotive SoCs. Designers of this new class of ADAS SoCs rely on IP suppliers to help overcome the challenges of implementing the automotive application-specific IP requirements including the ISO 26262 functional safety standard.

This white paper describes the new ADAS SoC architecture which has transitioned from decentralized ECUs to centralized multi-domain controllers and explains the implementation of domain controllers with IP that has been designed per the ISO 26262 functional safety, automotive reliability, and quality standards.

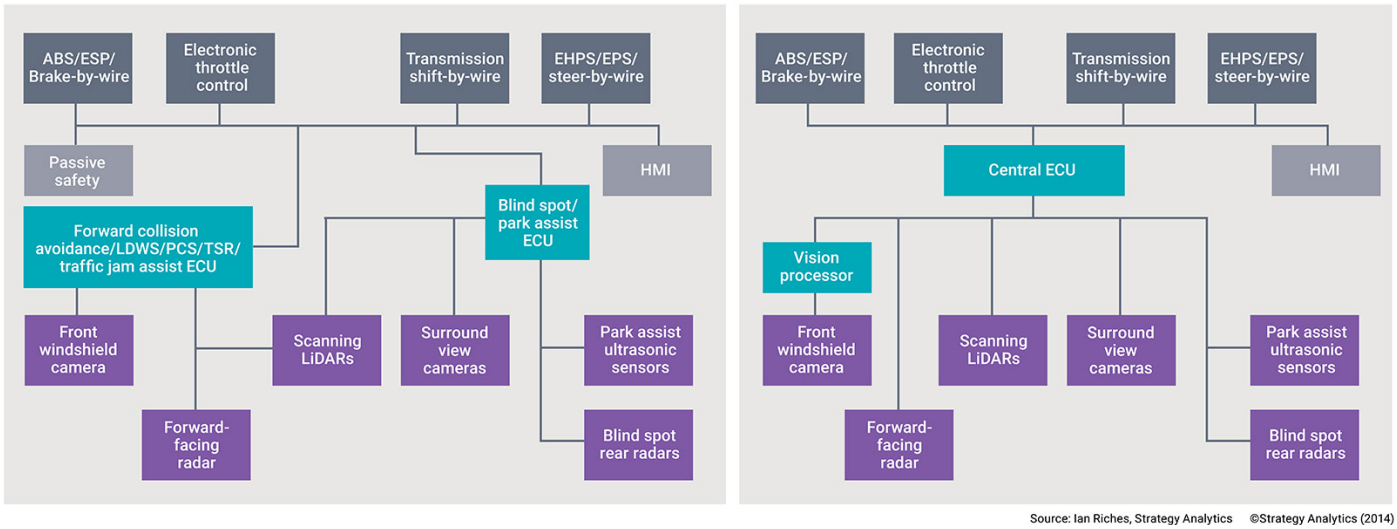


Figure 2: Current and future ADAS system architectures from distributed ECUs to centralized domain controllers

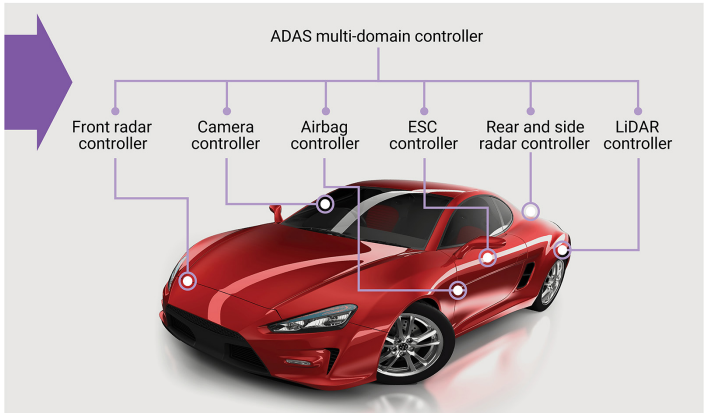


Figure 3: Aptiv (formerly Delphi) ADAS multi-domain controller

ADAS Processors for Multi-Domain Controllers

Centralized ADAS architectures will require a new generation of high performance 32-bit or 64-bit processors running at clock frequencies over 1 GHz. For example, ADAS SoCs that support multiple vision-based applications are using 64-bit processors with separate processor accelerators to implement latest deep learning algorithms such as Convolutional Neural Networks (CNN).

An additional graphics processor or customized DSP core handles high-rate pixel processing connected to a multimedia interface such as HDMI or MIPI D-PHY, which together support the increasingly large high-definition displays. To support the multiple camera and radar sensors supplying image and radar/LIDAR data, a sensor and control subsystem that offloads the application processor from sensor data management duties will enable the high degree of sensor fusion.

The new generation of ADAS SoCs requires up to 8GB automotive-grade LPDDR4 memory to support the processor application software and extensive system connectivity provided by Ethernet with Time Sensitive Networking (TSN) to support multimedia data traffic. PCI Express and new cache coherent interfaces such as Cache Coherent Interconnect for Accelerators (CCIX) have become popular to connect multiple processors for scalable applications. Various SoC peripherals such as MIPI I3C, I2C, UARTs, SPI/QSPI , CAN, and FlexRay offer additional interface connectivity. The adoption of MIPI I3C is increasing due to its two-wire interface and data rates up to 33.4 Mbps.

To support cloud connectivity enabled by an external Bluetooth Low Energy, WiFi or 4G LTE radio IC, the ADAS SoC must include robust hardware-based security protocols for secure boot, secure identification and authentication, encryption, and decryption. Figure 4 shows a high performance ADAS processor architecture in leading edge process technology.

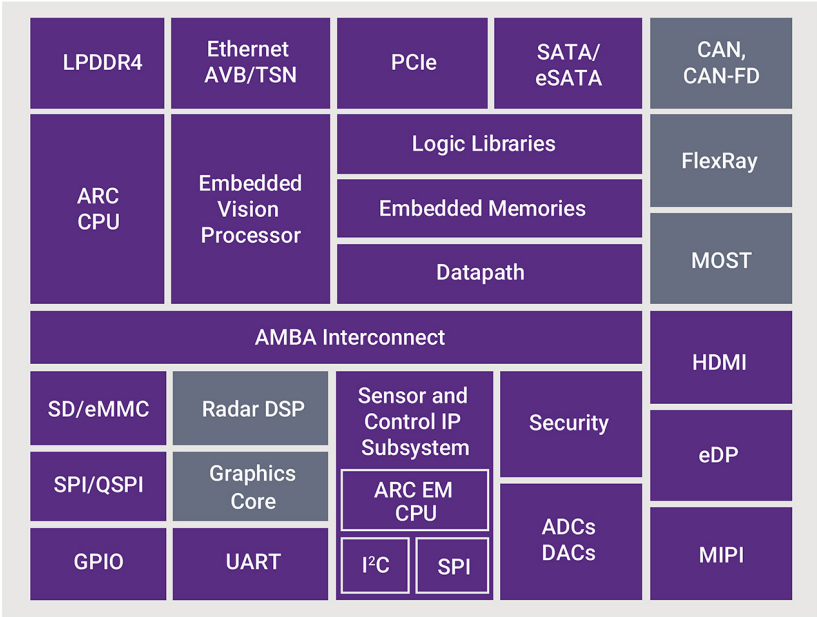


Figure 4: ADAS processor architecture for multi-domain controller

IP for ISO 26262 ASIL Ready Functional Safety

Centralized domain controller SoCs for ADAS safety-critical applications require IP functions supporting the latest specifications and algorithms in leading foundry processes. In addition to providing the required advanced features, small area, high performance and low power for ADAS SoCs, IP suppliers must meet the automotive ISO 26262 functional safety standard. The ISO 26262 standard, which was released in 2011 and updated in 2018, applies to functional safety in electrical and/or electronic systems within road vehicles. It addresses all activities of the safety lifecycle such as design and development of safety-related systems, and includes SoCs that are classified as Safety-Elements-out-of-Context (SEooC). ISO 26262 provides an automotive-specific approach for determining Automotive Safety Integrity Levels (ASIL) and specifies measures to validate and confirm that the safety levels are achieved. The goal is to minimize susceptibility to random hardware failures by defining functional requirements, applying rigor to the development process and taking the necessary design measures including fault injection and systemic analysis and metrics reporting. Using IP that has been ISO 26262 certified will help SoC designers reduce supply chain risk and accelerate the requirements specification, design, implementation, integration, verification, validation, and configuration of SoC-level functional safety.

Synopsys' IP development organization implements the policies, processes, strategies and management required for ASIL Ready IP. In addition to the detailed functional safety training for development engineering, Synopsys' safety managers have received intense training and certification as Semiconductor Automotive Functional Professionals (SC-AFSP) by leading automotive inspection company SGS-TUV Saar and are fully empowered to ensure that the IP development adheres to the requirements.

As seen in Figure 5, the Synopsys IP development flow includes ISO 26262 work products,which provides integrated hardware safety features, verification plans, safety plans, verification reports, safety manuals and Failure Mode Effect and Diagnostic Analysis (FMEDA). The Synopsys IP automotive safety packages contain the deliverables which enable SoC designers to develop their SoC-level FMEDA report, thereby accelerating their SoC development. Compliance certifications for SoCs and IP as SEooCs elements are granted by accredited industry auditors such as SGS-TUV Saar who perform product and process reviews, assessments and audits of functional safety elements including ISO 26262 Work Products such as safety plans, safety features, Failure-in-Time (FIT) rate analysis, and FMEDA analysis.

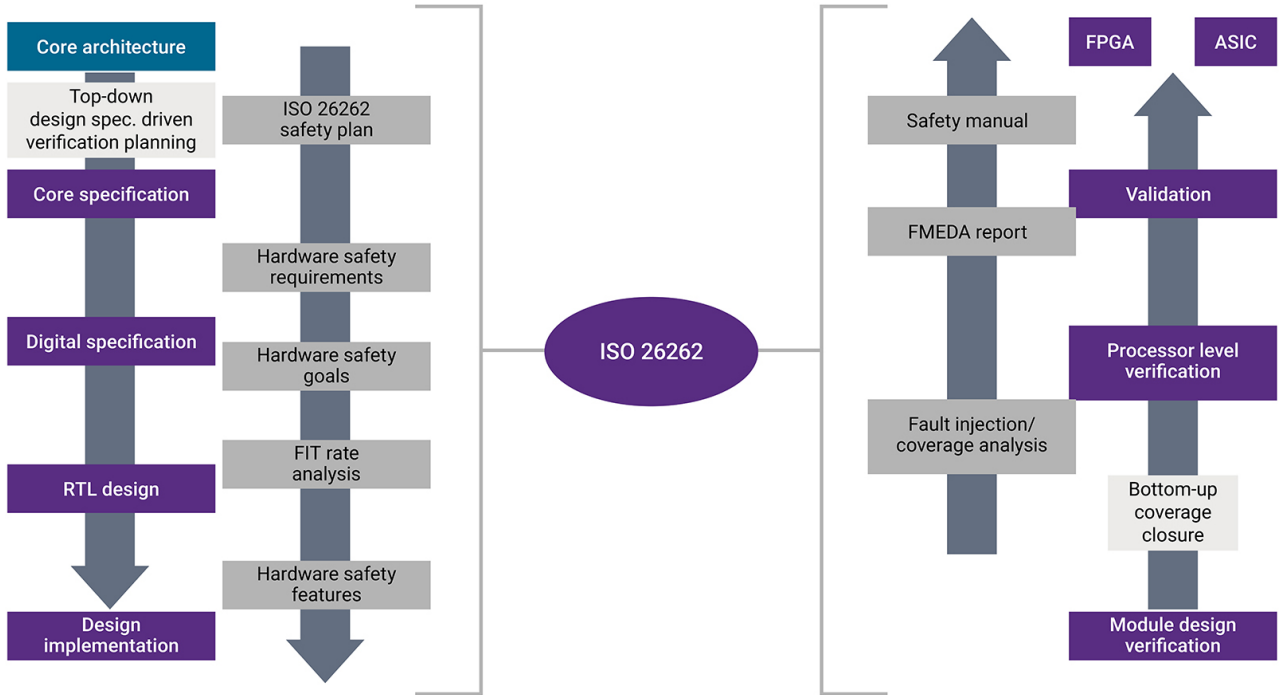


Figure 5: Synopsys IP development includes functional safety work products

Best Practices: IP for ISO 26262 ASIL Ready Functional Safety

With experience in delivering IP with automotive safety packages, Synopsys has defined several best practices for automotive product development:

1. Participation by safety managers in each stage of the IP development, including process audits, with concurrent reviews performed by multiple engineers to eliminate bias
2. Implementation of specific-functional safety features into the IP
3. Documentation for each key specification and decision as part of requirements tracing by an assigned team member
4. Analysis of the IP—block-by-block—as part of the ASIL assessment using the FMEDA report, where the IP designer must identify all the possible failure modes for each of the blocks and the error detection/diagnostics/corrections for these failure modes (random faults)

Synopsys implements safety features into our IP products based on multiple criteria including recommendations from the ISO 26262 standard. A summary of recommendations and impact of those features for the product are shown in Table 1.

Safety Feature Type	Effectiveness
HW redundancy	High–99%
Configuration register test	High–99%
EDC* on memory	High–99%
Combination of timeout monitoring, frame counter & information redundancy	High–99%
Self-test supported by hardware	High–99%
Multi-bit HW redundancy	Medium–90%
Timeout monitoring	Medium–90%
Frame counter	Medium–90%
Information redundancy	Medium–90%
Parity bit–per word	Low–60%

Table 1: Synopsys' IP implements safety features as per the ISO 26262 standard's recommendations

Synopsys' IP solutions implement multiple safety features to mitigate impact of random errors. The set of safety features implemented in the automotive IP products include such functionality as error-correcting code (ECC) protection for packet headers, data path parity, ECC for closely coupled memories, configuration register parity and triple modular redundancy for critical functions. In addition to safety functionality for improving automotive IP solution's ability to reduce random errors, the products contain a variety of internal and external diagnostics which allow the products to communicate to the system software to provide ongoing safety status. The combination of functional safety features and diagnostics enable the complex IP in ADAS SoCs to operate in safety-critical applications.

In addition to the safety functions and diagnostic coverage metrics contained in the IP solution's FMEDA report, a complete FIT rate calculation is performed.

The FIT rate calculation in FMEDA development include:

- Use of industry standard Siemens SN 29500 failure rates
- Use of failure rate lambda values defined in IEC TR 62380, as shown in Figure 6

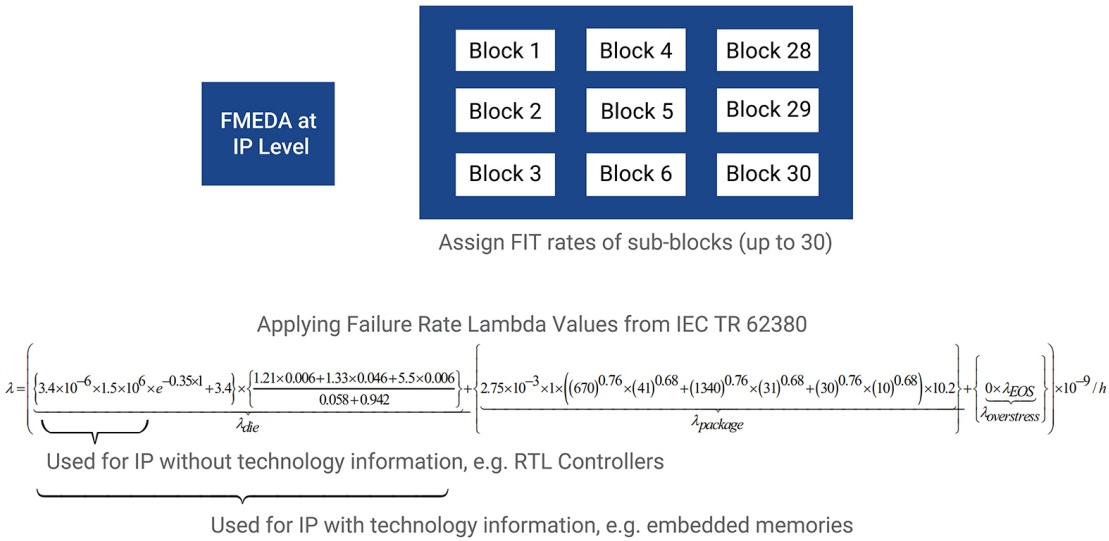
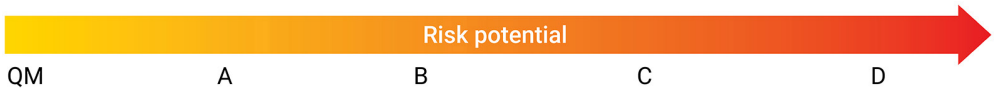


Figure 6: FIT rate calculations as part of FMEDA IP assessment

After the detailed failure rate and diagnostic analysis is complete, the Automotive Safety Integrity Level (ASIL) metric is determined based on the ISO 26262 risk potential. Table 2 shows the various ASIL levels based on fault coverage metrics.



QM	Not used for safety			
ASIL A	NA		ASIL C	Single-point fault metric > 97% Latent fault metric > 80%
ASIL B	Single-point fault metric > 90% Latent fault metric > 60%		ASIL D	Single-point fault metric > 99% Latent fault metric > 90%

Table 2: ASIL based on coverage metrics

Providing a complete automotive safety package for IP enables SoC designers to meet SoC-level safety goals. To ensure Synopsys IP deliverables and design flow meet designer requirements, Synopsys takes the extra step to obtain ISO 26262 certification by an industry accredited automotive safety inspection firm like SGS-TUV Saar. By obtaining ISO 26262 certification and receiving independent validation of ASIL Ready status, Synopsys reduces designer risk by ensuring our DesignWare® IP meets industry standards.


CERTIFICATE NO.: FS/71/220/16/0126

Figure 7: Example ISO 26262 Certificate for Synopsys IP: Embedded Memory Compilers

Synopsys' ASIL Ready ISO 26262 certified DesignWare IP portfolio is listed in Table 3. For the latest list of Synopsys' certified IP, visit synopsys.com/ip-automotive.

DesignWare IP	ASIL Functional Safety Certification
ARC EM SEP	ASIL D
ARC EM Safety Island	ASIL D
EV Vision Processors	ASIL D
Embedded Memories 16FFC	ASIL D
STAR Memory System	ASIL D
STAR Hierarchical System	ASIL D
NVM	ASIL D
Ethernet QoS (AVB/TSN)	ASIL B
PCI Express 4.0 Controller, PCIe 3.1 Controller and 16FFC PHY	ASIL B
USB 3.0 Controller	ASIL B
LPDDR4 Controller and MultiPHY v2	ASIL B
MIPI CSI-2 Controller and 16FFC PHY	ASIL B
Sensor and Control Subsystem	Compliance in progress or planned
Security IP	Compliance in progress or planned

Table 3: List of Synopsys' ASIL Ready ISO 26262 certified IP portfolio

Best Practices: IP for AEC-Q100 Reliability

In addition to meeting ISO 26262 functional safety requirements, centralized domain controller SoCs for ADAS safety critical applications operate in harsh automotive environments with 15-year product lifetimes. The SoCs and the complex IP used in the SoCs must be designed per the reliability requirements of the automotive industry. It is not possible to repurpose consumer-based IP to meet the robust operating environments of centralized domain controller SoCs. The IP blocks in the SoCs need to be designed, verified, and tested for high-reliability. Since the IP blocks will operate under specific temperature profiles, the IP must be designed based on end product temperature profiles defined by the end application. Synopsys has defined automotive temperature profiles to which IP development teams design and verify the IP blocks. Using foundry-specific automotive design manuals, tech files and design rule checks (DRCs), the IP blocks must take into account the impact of current electromigration, transistor aging and transistor self-heating which occur over time. By designing the IP blocks based on high-reliability and low defect densities, the IP is designed to be more robust compared to commercial IP. While designing and verifying the IP based on high reliability automotive requirements is an integral part of product development, testing the IP products per the automotive reliability standard is an additional requirement. Synopsys GDSII-based automotive IP products are tested according to relevant Automotive Electronics Council AEC–Q100 Rev H (Sep, 2014) automotive stress test qualification for integrated circuits. Not all AEC-Q100 tests apply to IP blocks, such as package qualification. By passing tests which do apply to IP blocks increases the likelihood that the SoC will pass AEC–Q100 qualification since the IP modules have been tested per the AEC -Q100 standard.

Best Practices: Quality Management System

Safety and reliability are critical requirements for centralized domain controller SoCs. In addition to safety and reliability, the ADAS SoCs must be developed according to the automotive Quality Management System (QMS) requirements. Systematic design processes used in the development of automotive IP products must meet the requirements specified under the ISO 9001 and relevant sections of International Automotive Task Force (IATF) 16949 QMS standards. Milestone tracking, specification traceability, reporting, monitoring, and systematic audits must occur to ensure the products are developed to meeting the high quality requirements of the automotive industry.

Summary

IP suppliers play a key role in the automotive supply chain to enable the new generation of centralized domain controller ADAS SoCs. For example, vision-based SoCs may contain a high amount of third-party IP to implement the key embedded vision, sensor fusion, multimedia, security, and advanced connectivity functions. Although IP suppliers have permeated the semiconductor ecosystem for consumer, mobile, PC, and communications applications, not all IP suppliers can support stringent automotive-level requirements. As designers initiate their next-generation ADAS SoCs, they must assess the IP suppliers' capability to provide ISO 26262 safety packages with ISO 26262 certification. IP suppliers with the commitment and resources to meet automotive industry requirements help ensure the success of automotive SoC suppliers, Tier 1s, and OEMs to meet the functionality, performance, quality, and reliability levels for ADAS SoCs targeting 28-nm, and 16-/14-nm, 7-/8-nm FinFET technologies.

For information on Synopsys' DesignWare IP portfolio for automotive SoCs, please visit www.synopsys.com/ip-automotive.

References:

[1] National Motor Vehicle Crash Causation Survey, NHTSA, February 2015
[2] CES 2018 Strategy Presentation, Dr Elmar Degenhart, CEO, Continental

SYNOPSYS®
Silicon to Software™

06/19/18.CS12655_ADAS Domain Controller_WP.
Pub: May. 2018