

UNIVERSIDAD AMERICANA
FACULTAD DE INGENIERÍA & ARQUITECTURA



“Análisis de Seguridad y Evaluación de Riesgo para el Sistema Avanzado de Asistencia al Conductor en Vehículos Volvo”.

Adiac Ernesto Aguilar González

Monografía para optar por el título de

Ingeniero Industrial

Tutor: M.Sc. Marlon Velásquez Reynosa

Managua, Nicaragua

Noviembre, 2020



Análisis de Seguridad y Evaluación de Riesgos para el Sistema Avanzado de Asistencia al Conductor - ADAS

Una auditoría de seguridad en la fase conceptual del vehículo para la presentación de metas de seguridad funcional.

Adiac E. Aguilar González

Facultad de Ingeniería y Arquitectura

Trabajo Monográfico para el grado de Ingeniería Industrial

UNIVERSIDAD AMERICANA UAM

Managua, Nicaragua 2020



Monografía de Ingeniería Industrial 2020

“Análisis de Seguridad y Evaluación de Riesgo para el Sistema Avanzado de Asistencia al Conductor - ADAS”.

Auditoría de seguridad en la fase conceptual para la presentación de metas de seguridad funcional.

Adiac E. Aguilar G.

Approved 2020 - 05 - 31	Tutor Marlon Velásquez	Coordinadora de Carrera Priscilla González
	Facultad Facultad de Ingeniería y Arquitectura	Decana de Facultad Raquel Hurtado

© ADIAC E. AGUILAR GONZÁLEZ, 2020

Licenciatura en Ciencias - Ingeniería Industrial 2020

NIIF 16010234

Facultad de Ingeniería y Arquitectura

Carrera de Ingeniería Industrial

Universidad Americana UAM

SE 21 AV, Managua

Telephone: +46 72 165 1169

Cover: Guided by laser - How Autonomous Cars see (Volvo Cars)

Fuente: Arial

Managua, Nicaragua 2020

AGRADECIMIENTOS

Me gustaría agradecer a todos/as los que tuvieron un rol en mis logros académicos. En especial a mi familia, quien me ha apoyado incondicionalmente durante este trayecto académico y han cultivado en mí, las ansías de expandir mis conocimientos con el fin de aportar sosteniblemente al desarrollo de la humanidad.

Quisiera expresar mi agradecimiento a mi tutor de investigación, el profesor Marlon Velásquez, quien transmitió de manera continua y convincente un espíritu de aventura en lo que respecta a la investigación. Su notable ilusión en la enseñanza, son características que promueven el espíritu de investigación. Su guía y ayuda persistente ha hecho posible la culminación de esta tesis.

Un especial agradecimiento a todos los miembros del comité involucrados de Volvo Cars & Zenuity en esta investigación, por guiarme constantemente con sus experiencias en el campo de vehículos autónomos y permitirme colaborar con el departamento de Seguridad Funcional, pese las circunstancias extraordinarias de la actual pandemia, COVID 19.

One new idea leads to another, that to a third a so on through a course of time, until someone, with whom no one of these ideas was original, combines all together and produces what is justly called a new invention

- Thomas Jefferson

ÍNDICE

AGRADECIMIENTOS	7
TÉRMINOS Y ABREVIATURAS	14
LISTA DE FIGURAS	16
LISTA DE TABLAS	17
RESUMEN	18
1. INTRODUCCIÓN	19
2. ANTECEDENTES	20
2.1 LA CARGA GLOBAL DE MUERTES POR ACCIDENTES DE TRÁFICO	21
2.2 ESTADO DEL ARTE DE LA SEGURIDAD AUTOMOTRIZ	24
2.3 SEGURIDAD AUTOMOTRIZ: ISO 26262	24
2.4 ELECTRÓNICA AUTOMOTRIZ.....	25
2.5 REVISIÓN BIBLIOGRÁFICA.....	27
3. JUSTIFICACIÓN	31
4. OBJETIVOS	32
OBJETIVO GENERAL	32
OBJETIVOS ESPECÍFICOS	32
5. MARCO TEÓRICO	33
5.1 DEFINICIÓN DEL SISTEMA ADAS.....	33
5.2 COMPONENTES DE ADAS.....	34
5.2.1 SISTEMA ANTIBLOQUEO DE FRENOS	34
5.2.2 CONTROL DE ESTABILIDAD ELECTRÓNICO	35
5.2.3 SISTEMA DE CONTROL DE TRACCIÓN	36
5.2.4 CONTROL DE CRUCERO Y CONTROL ADAPTATIVO	37
5.2.5 AVISO DE COLISIÓN FRONTAL Y FRENADO DE EMERGENCIA AUTÓNOMA	38
5.2.6 SUPERVISIÓN DE PUNTOS CIEGOS / ASISTENCIA DE CAMBIO DE CARRIL.....	39

5.2.7 AVISO DE SALIDA DE CARRIL / AYUDA DE MANTENIMIENTO DE CARRIL	40
5.2.8 SENSOR DE ESTACIONAMIENTO / SISTEMA DE ASISTENCIA DE ESTACIONAMIENTO	41
5.2.9 ALERTA DE TRÁFICO CRUZADO	42
5.2.10 ASISTENCIA DE GIRO	44
5.2.11 GLARE - FREE HIGH BEAM	45
5.2.12 SISTEMA DE NAVEGACIÓN AUTOMOTRIZ	46
5.2.13 VISIÓN NOCTURNA AUTOMOTRIZ	47
5.2.14 ESTABILIZACIÓN DE VIENTO CRUZADO	48
5.2.15 ADAPTACIÓN DE VELOCIDAD INTELIGENTE (ISA)	48
5.2.16 SURROUND VIEW SYSTEM	49
5.2.17 SISTEMA DE CONTROL DE PRESIÓN DE NEUMÁTICOS	50
5.2.18 SISTEMA DE MONITOREO DEL CONDUCTOR	50
5.2.19 SISTEMA DE SONIDO DE ADVERTENCIA DE VEHÍCULOS ELÉCTRICOS	51
5.2.20 CONTROL DE DESCENSO EN PENDIENTES	53
5.2.21 RECONOCIMIENTO DE SEÑALES DE TRÁFICO	54
5.3 SENSORES DE ADAS	55
5.3.1 RADAR	56
5.3.2 SENSOR DE VIDEO	58
5.3.3 LIDAR	62
5.3.4 SENSORES ULTRASÓNICOS	64
5.3.5 COMUNICACIÓN INALÁMBRICOS	66
5.3.6 FUSIÓN DEL SENSOR	66
5.4 NIVELES DE AUTOMATIZACIÓN	68
5.4.1 NIVEL 0	69
5.4.2 NIVEL 1	69
5.4.3 NIVEL 2	69
5.4.4 NIVEL 3	70
5.4.5 NIVEL 4	70
5.4.6 NIVEL 5	70
5.5 CICLO DE VIDA Y SEGURIDAD AUTOMOTRIZ	74
5.5.1 PARTE 1	76

5.5.2 PARTE 3	78
5.5.3 PARTE 3 ISO 26262: "METODOLOGÍA"	87
5.5.4 SISTEMA Y SEGURIDAD PARA LA FASE DE CONCEPTO.....	88
6. METODOLOGÍA.....	89
6.1 MATERIAL Y MÉTODO.....	89
6.2 TIPO DE ESTUDIO.....	89
6.3 DEFINICIÓN OPERACIONAL DE LAS VARIABLES	90
6.4 POBLACIÓN Y MUESTRA	91
6.5 INSTRUMENTOS DE RECOLECCIÓN DE DATOS	91
6.5 ANÁLISIS Y PROCESAMIENTO DE LA INFORMACIÓN	92
7. RESULTADOS Y DISCUSIÓN.....	95
7.1 FMEA.....	95
7.1.1 CRITERIOS DE PRIORIDAD DE RIESGO.....	96
7.1.2 MATRIZ DE RIESGO	99
7.1.3 PROCESO FMEA	105
7.2 HARA.....	107
7.2.1 DEFINICIÓN DE ÍTEMS.....	107
7.2.2 ANÁLISIS SITUACIONAL E IDENTIFICACIÓN DE PELIGROS	116
7.2.3 HAZOP	125
7.2.4 CLASIFICACIÓN DE EVENTOS PELIGROSOS	137
7.2.5 DETERMINACIÓN DE OBJETIVOS DE SEGURIDAD	142
7.2.6 REQUISITOS DE SEGURIDAD FUNCIONAL	151
8. CONCLUSIONES	152
9. RECOMENDACIONES.....	154
REFERENCIAS BIBLIOGRÁFICAS	156
ANEXOS.....	162

TÉRMINOS Y ABREVIATURAS

ABS	Anti - Lock Braking System
ACC	Adaptive Cruise Control
AD	Autonomous Driving
ADAS	Advanced Driver Assistance System
AEB	Autonomous Emergency Braking
AI	Artificial Intelligence
ASIL	Automotive Safety Integrity Level
AVAS	Acoustic Vehicle Alert System
AUTOSAR	Automotive Open Source Architecture
BAST	Federal Highway Research Institute (Germany)
BCM	Body Control Module
CAN	Controller Area Network
CCD	Charge Coupled Device
CFT	Cross Functional Team
CTA	Cross Traffic Alert
DMS	Driver Monitoring System
ECU	Electronic Control Unit
ECM	Electronic Control Module
ESA	Evasive Steering Assist
ESC	Electronic Stability Control
ESP	Electronic Stability Program
EPS	Electronic Power Steering
EV	Electric Vehicle
FCW	Forward Collision Warning
FIR	Far Infra-Red
FMEA	Failure Mode Effective Analysis
FSRA	Full Speed Range Adaptive Cruise Control
FTA	Fault Tree Analysis
FTTI	Fault Time Tolerance Interval
Functional Safety	Safety concerned with changes in the environment, hardware failure, correct input response and likely errors caused by the operator of a system.
FuSa	Functional Safety
GS	Global shutter
GPS	Global Positioning System
HAZOP	Hazard and Operability Study
HARA	Hazard and Risk Analysis
HDC	Hill Descent Control
HEV	Hybrid Electric Vehicles
HMI	Human Machine Interface
HUD	Head Up Display
IC	Integrated Circuit
ICE	Internal Combustion Engine
ISA	Intelligent Speed Adaptation
LDW	Lane Departure Warning
LED	Light Emitting Diode
LiDAR	Light Detection & Ranging
LKAS	Lane Keeping Assist System
LRR	Long Range Radar
MRR	Medium Range Radar
NHTSA	National Highway Traffic Safety Administration
NIR	Near Infra-Red
NPR	Número de Prioridad de Riesgo

OEM	Original Equipment Manufacturers
PCM	Powertrain Control Module
PHA	Preliminary Hazard Analysis
PHEV	Plug – in Hybrid Electric Vehicle
QA	Queue Assist
RADAR	Radio Detection and Ranging
RDM	Road Departure Mitigation
R&D	Research & Development
SAE	Society of Automotive Engineers
SRR	Short Range Radar
STPA	Systematic Theoretic Process Analysis
TCM	Transmission Control Module
TCS	Traction Control System
TSR	Traffic-sign recognition
UCA	Uncontrolled Control Actions
ULTRASONIC	Sound waves with frequencies higher than the upper audible limit of human hearing.
VC	Vehicle Control
V2V	Vehicle to Vehicle
V2I	Vehicle to Infrastructure

LISTA DE FIGURAS

- Figura 1** Tasa de mortalidad por accidentes de tránsito por 100.000 habitantes. WHO (2016)
- Figura 2** Principales causas de accidentes en Europa. NHTSA (2016)
- Figura 3** Diferentes ECU de un automóvil moderno. FEV (2013)
- Figura 4** Diagrama de funcionalidad de ABS. Jitesh (2014)
- Figura 5** Funcionalidad de control electrónico de estabilidad. (NHTSA (2020)
- Figura 6** Funcionalidad del sistema de control de tracción. ISO 7000:2045 (2004)
- Figura 7** Control de crucero adaptativo en vehículos Volvo. Volvo Cars AB (2018)
- Figura 8** Advertencia de colisión frontal, Volvo Cars AB (2014)
- Figura 9** Frenado de emergencia autónomo, Volvo Cars AB (2018)
- Figura 10** Sistema de asistencia a la decisión de cambio de carril, Volvo Cars AB (2018)
- Figura 11** Sistema Volvo de advertencia de cambio de carril, Volvo Cars AB (2018)
- Figura 12** Detección de puntos del sistema de asistencia de estacionamiento, Volvo Cars AB (2018)
- Figura 13** Icono de CTA en el gráfico de asistencia de estacionamiento del monitor, Volvo Cars AB (2020) actualizado en 2020.
- Figura 14** Sistema de Asistencia de Giro, NEOPLAN (2020)
- Figura 15** Sistema Glare - free High Beam, Bosch (2017)
- Figura 16** Sistema de Navegación GPS de Vehículos, Volvo Cars AB (2020)
- Figura 17** Estabilización de Viento Cruzado, Daimler (2014)
- Figura 18** Adaptación de Velocidad Inteligente, EU Commission for Mobility & Transport (2016)
- Figura 19** Surround View System, Volvo Cars AB (2020)
- Figura 20** Alerta de Presión de Neumáticos, Volvo Cars AB (2017)
- Figura 21** Detección de Somnolencia del Conductor, Bosch (2018)
- Figura 22** Sistema Acústico de Advertencia, Bosch (2018)
- Figura 23** Control de Descenso en Pendientes, Volvo Cars AB (2015)
- Figura 24** Reconocimiento de Señales de Tráfico, Volvo Cars AB (2016)
- Figura 25** Funciones y sensores ADAS, (SAE 2016)
- Figura 26** Fusión del sistema de radar en ADAS, Texas Instruments (2018)
- Figura 27** Fusión del sistema de cámara en ADAS, Texas Instruments (2018)
- Figura 28** Fusión del sistema LIDAR en ADAS, Texas Instruments (2018)
- Figura 29** Fundamentos de la detección ultrasónica, Stiawan (2019)
- Figura 30** Fusión del sistema ultrasónico en ADAS, Texas Instruments (2018)
- Figura 31** Sistema de fusión de sensores en ADAS, Texas Instruments (2018)
- Figura 32** Árbol de objetivos para el sistema ADAS, basado en Alexander (2011)
- Figura 33** Objetivos operativos y sus funciones preliminares con base en la tabla 3
- Figura 34** Modelo V para el proceso del ciclo de vida del sistema, Administración Federal de Carreteras (2007)
- Figura 35** S, C y E según, ISO 26262 (2018)
- Figura 36** Seguridad a través de medidas externas basadas en ISO 26262 (2018)
- Figura 37** Metodología de la fase conceptual de ISO 26262, basada en ISO 26262 (2018)
- Figura 38** Metodología de ciclo de vida de seguridad e ingeniería de sistemas derivados, basada en ISO 26262 (2018)
- Figura 39** Relación entre ítems y elementos externos por medio de CAN
- Figura 40** Límite de interacción del ítem
- Figura 41** Eventos Peligrosos - Desvinculación en Curva
- Figura 42** Eventos Peligrosos - Detección de Señales Horizontales y Múltiples Objetos
- Figura 43** Eventos Peligrosos - Situaciones Climáticas
- Figura 44** Eventos Peligrosos - Escenarios Urbanos
- Figura 45** Resumen de Eventos Peligrosos
- Figura 46** Relación de Ítems con Requisitos de Seguridad Funcional

LISTA DE TABLAS

Tabla 1	Asistencia de las funcionalidades de ADAS sobre limitaciones humanas, EU Commission Mobility and Transport of Road Safety (2020)
Tabla 2	Niveles SAE de fuente de automatización, Smith Bryant Walker, Stanford (2013)
Tabla 3	Niveles SAE de fuente de automatización, SAE J3016 (2018)
Tabla 4	Resumen del capítulo, ISO 26262 (2018)
Tabla 5	Glosario de ISO 26262 (2018)
Tabla 6	Tabla de gravedad basada en ISO 26262 (2011)
Tabla 7	Tabla de exposición basada en ISO 26262 (2018)
Tabla 8	Tabla de controlabilidad basada en ISO 26262 (2018)
Tabla 9	Guía de determinación de ASIL basada en ISO 26262 (2018)
Tabla 10	Escala genérica de gravedad de cinco puntos, Bluvband & Grabov (2009)
Tabla 11	Escala genérica de ocurrencia de cinco puntos, Bluvband & Grabov (2009)
Tabla 12	Escala genérica de detección de cinco puntos, Bluvband & Grabov (2009)
Tabla 13	Matriz de Riesgo Desvinculación del Sistema al tomar Curvas
Tabla 14	Matriz de Riesgo Señales Horizontales y MOT
Tabla 15	Matriz de Riesgo Situaciones Climáticas
Tabla 16	Matriz de Riesgo Ambiente Urbanos
Tabla 17	FMEA Proceso - ADAS
Tabla 18	Modos de funcionamiento y estado del ítem
Tabla 19	Caso de Uso Desvinculación del sistema al tomar curvas
Tabla 20	Caso de Uso Mal interpretación de líneas de tráfico horizontales
Tabla 21	Caso de Uso Situaciones Climáticas
Tabla 22	Caso de Uso Ambientes Urbanos
Tabla 23	Parametrización de Severidad
Tabla 24	Parametrización de Exposición
Tabla 25	Parametrización de Controlabilidad
Tabla 26	ASIL Categorización de eventos peligrosos, ISO 26262 (2011)
Tabla 27	ASIL Desvinculación del sistema al tomar curvas o giros
Tabla 28	ASIL Falla de detección de señales horizontales y de múltiples objetos
Tabla 29	ASIL Situaciones Climáticas
Tabla 30	ASIL Ambiente Urbano
Tabla 31	Objetivos de Seguridad: Desvinculación del sistema al tomar curvas
Tabla 32	Objetivos de Seguridad: Fallo de detección de señales horizontales y MOT
Tabla 33	Objetivos de Seguridad: Situaciones Climáticas
Tabla 34	Objetivos de Seguridad: Ambientes Urbanos
Tabla 35	Matriz Operacional de Variables

RESUMEN

Los fabricantes de equipos originales de la industria del automóvil (OEM) buscan constantemente formas de incorporar y mejorar las funcionalidades de Sistema Avanzado de Asistencia al Conductor (ADAS) en sus vehículos. El propósito de esta tesis es estudiar el sistema actual de ADAS presente en vehículos Volvo, diseño y arquitectura del tal, ha sido producido por Zenuity. Se identificarán y analizarán los peligros potenciales que podrían resultar de los casos de fallos eléctricos o electrónicos que afecten las funciones de los sistemas de control vehicular. El estudio sigue el proceso ISO 26262 para identificar los requisitos de integridad de estas funciones a nivel de la fase de concepto, independientemente de las variaciones de implementación. Este estudio también considera las causas potenciales que podrían conducir a tales fallas funcionales y documenta los requisitos técnicos que sugiere el proceso ISO 26262 con respecto al nivel de riesgo identificada del ítem en consideración. Si bien este estudio no analiza las estrategias de implementación para lograr los niveles de integridad de seguridad automotriz (ASIL), el proceso ISO 26262 proporciona un marco flexible y una guía explícita para que los fabricantes busquen diferentes métodos y enfoques para hacerlo. Los fabricantes emplean una variedad de técnicas, como descomposiciones ASIL, advertencias a los conductores, mecanismos de detección de fallas, verificaciones de plausibilidad, redundancias, etc., para lograr los ASIL necesarios que mitigan de manera efectiva los riesgos de seguridad subyacentes. La presente investigación concluye en el logro de clasificar el nivel de riesgo de los eventos peligrosos ASIL, y la identificación de los causas de fallas a nivel de sistema lo que permite analizar los efectos que provocan tales fallas y brindar recomendaciones generales de manera individual, como medidas para mitigar dichas fallas. El resultado del análisis es la elaboración de objetivos de seguridad para cada uno de los ítems, los cuales posteriormente se traducen en requisitos de seguridad funcional en las siguientes etapas de desarrollo.

Palabras clave: ISO 26262, HARA, seguridad funcional, análisis de seguridad, ADAS, fase conceptual, FMEA, ASIL.

1. INTRODUCCIÓN

En los últimos seis años ha resurgido el tema de desarrollo de los vehículos autónomos y se ha notado un interés por parte de las distintas OEMs para implementar estas tecnologías en los sistemas actuales de los vehículos. La Sociedad de Ingenieros Automotrices (SAE) define cinco niveles de automatización y autonomía, cada nivel requiere menor grado de intervención humana. Muchos expertos concluyen que para llegar a los niveles más altos de autonomía (Niveles 4 - 5), se requiere establecer una base de seguridad operacional del sistema en distintos escenarios peligrosos e inusuales para poder cumplir con los objetivos de seguridad funcional en los niveles más bajos (Niveles 1 - 3). Siendo entre de los mayores puntos de discusión, la seguridad y el riesgo que estos sistemas pueden experimentar, poniendo en riesgo al conductor. Volvo Cars es una subsidiaria de la empresa automotriz Zhejiang Geely Holding Group Co. Ltd. Volvo es conocida por inventar el cinturón de seguridad de tres punto, siendo la seguridad uno de los principales enfoques de la empresa. Los sistemas ADAS actuales de los vehículos Volvo es desarrollada por una subempresa llamada Zenuity / Ztwo en colaboración con la empresa Veoneer. Los vehículos manufacturados para la fecha (2020 - 2021) tienen un rango de automatización operacional nivel 2. Al igual que otras empresas automotrices que se encuentran en la competencia en desarrollar un sistema autónomo seguro y comercial, existen varios retos, entre ellos percepción, detección y rastreo de objetos múltiples, así como mitigar errores de componentes eléctricos / electrónicos que causan un mal funcionamiento del sistema. Este estudio se realizará en colaboración de Volvo & Zenuity / Ztwo, y se realizará un análisis de seguridad y riesgo mediante un análisis de modo de falla y efecto (FMEA) y un análisis de peligros y evaluación de riesgos (HARA), desde la ciudad de Gotemburgo, Suecia, donde se encuentran las sedes de ambas empresas, punto de centros de investigación y desarrollo.

2. ANTECEDENTES

Introducir la conducción autónoma de una vez sería demasiado peligroso y simplemente imposible, debido al extenso trabajo de investigación en seguridad funcional. Por este motivo, desde hace algunos años varios fabricantes de automóviles han comenzado a lanzar sus sistemas de asistencia paso a paso. Mediante este enfoque gradual, los sistemas se pueden probar en el entorno real. Al analizar la funcionalidad de sus componentes, se revelan posibles errores de desarrollo y, lo que es más importante, a menudo se encuentran casos que no fueron considerados. Como se mencionó anteriormente, los sistemas avanzados de asistencia al conductor (ADAS) y la conducción autónoma (AD) es una de las discusiones actuales más importantes en el sector de la tecnología automotriz. Los sistemas ADAS pueden proporcionar asistencia personal en un entorno vial que no siempre puede tener en cuenta las posibilidades y limitaciones de algunos conductores. Estas dificultades derivan de limitaciones funcionales como la disminución de la percepción del movimiento, la visión periférica, la flexibilidad del cuello, la atención selectiva y la velocidad de procesamiento de la información y la toma de decisiones. ADAS que puede compensar estas limitaciones, puede contribuir a reducir la participación de estos conductores en accidentes. Varios estudios han demostrado que ADAS puede brindar asistencia personalizada para los conductores, extendiendo las capacidades y reduciendo las dificultades resultantes de las limitaciones en la percepción del movimiento, la visión periférica, la atención selectiva y la disminución de la velocidad de procesamiento de la información y la toma de decisiones que se resumen en la siguiente tabla:

Funcionalidad	ADAS
Llama la atención sobre el tráfico que se acerca	<ul style="list-style-type: none"> • Sistemas de alerta de colisión dirigidos a intersecciones • Sistemas automatizados de cambio de carril e incorporación
Señala a los usuarios de la carretera ubicados en el punto ciego del conductor	<ul style="list-style-type: none"> • Sistemas automatizados de cambio de carril e incorporación • Sistemas de detección de obstáculos y puntos ciegos
Ayudar al conductor a dirigir su atención a la información relevante	<ul style="list-style-type: none"> • Sistemas de señalización de vehículos • Control de cruceo inteligente especial
Proporciona conocimientos previos sobre la próxima situación del tráfico	<ul style="list-style-type: none"> • Sistemas que brindan información sobre las características de intersecciones complejas que el conductor está a punto de cruzar

Tabla 1 Asistencia de las funcionalidades ADAS sobre limitaciones humanas, EU Commission Mobility and Transport of Road Safety (2020)

2.1 LA CARGA GLOBAL DE MUERTES POR ACCIDENTES DE TRÁFICO

Según (WHO, 2020) El número de muertes por accidentes de tránsito continúa aumentando de manera constante, alcanzando los 1,35 millones en 2016. Sin embargo, la tasa de muertes en relación con el tamaño de la población mundial se ha mantenido constante. Cuando se considera en el contexto del aumento de la población mundial y la rápida motorización que ha tenido lugar durante el mismo período, sugiere que los esfuerzos de seguridad vial existentes pueden haber mitigado el empeoramiento de la situación. Sin embargo, también indica que el progreso hacia la consecución de la meta 3.6 de los Objetivos de Desarrollo Sostenible (ODS), que exige una reducción del 50% en el número de muertes por accidentes de tránsito para 2020, está lejos de ser suficiente.

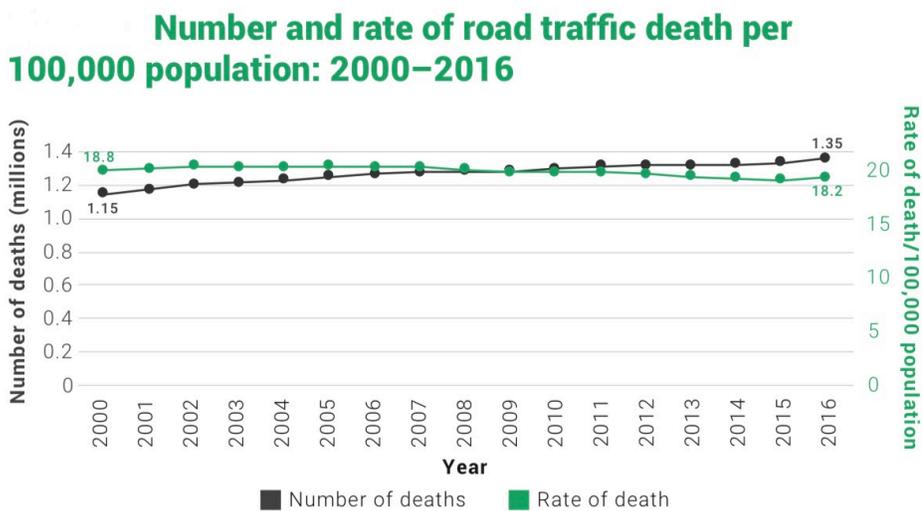


Figura 1 Tasa de mortalidad por accidentes de tráfico por 100.000 habitantes, World Health Organization (2016)

Ha aumentado la contribución relativa de las muertes por enfermedades no transmisibles y lesiones. Los traumatismos causados por el tránsito son la octava causa principal de muerte en todos los grupos de edad. Actualmente mueren más personas como consecuencia de los traumatismos causados por el tránsito que del VIH / SIDA, la tuberculosis o las enfermedades diarreicas. Los traumatismos causados por el tránsito son actualmente la principal causa de muerte de niños y adultos jóvenes de 5 a 29 años, lo que indica la necesidad de un cambio en la actual agenda de salud infantil y adolescente que, hasta la fecha, ha descuidado en gran medida la seguridad vial.

Según (NHTSA, 2017) El número de muertes en las carreteras del mundo sigue siendo inaceptablemente alto, con un estimado de 1,35 millones de personas que mueren cada año. La Administración Nacional de Seguridad del Tráfico en las Carreteras dice que "el 94% de los choques graves se deben a decisiones peligrosas o errores que cometen las personas al volante".

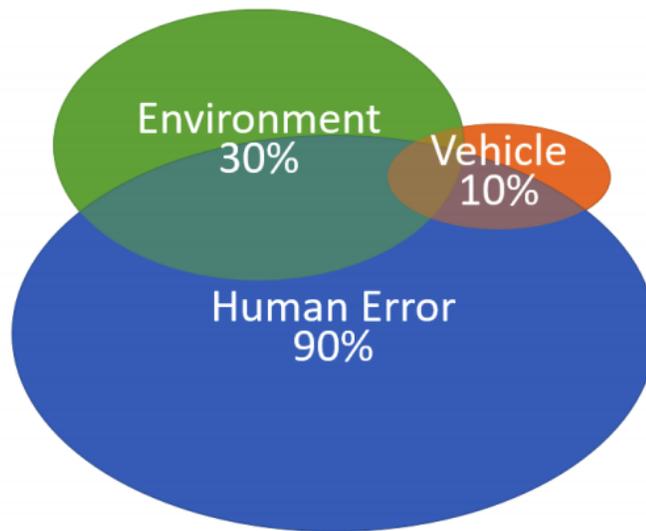


Figura 2 Principales causas de accidentes en Europa. NHTSA (2015)

En todo el mundo se está trabajando para un mayor desarrollo. Las nuevas innovaciones en esta área afectarán en gran medida el número de accidentes. Las estadísticas muestran que el principal factor de los accidentes de tráfico son los errores humanos, como la distracción, la velocidad o la conciencia del riesgo.

(NHTSA, 2015) Indica que los seres humanos son responsables de aproximadamente el 90% de los accidentes de tráfico, o al menos son corresponsables. Otras causas principales de accidentes son factores ambientales, como diseños de carreteras, clima, etc., con una cotización del 30 por ciento. Además de estos factores, alrededor del 10 % de las causas de accidentes corresponde a una falla a nivel del vehículo.

La razón principal de esta predicción es el mayor nivel de automatización en las calles. ADAS, que proporcionan funciones de seguridad automatizadas, están diseñadas para minimizar el error humano.

2.2 ESTADO DEL ARTE DE LA SEGURIDAD AUTOMOTRIZ

Según (Lundin, 2017) La seguridad de los vehículos es cada vez más crítica para la prevención de accidentes y se ha demostrado que contribuye a reducciones sustanciales en el número de muertes y lesiones graves resultantes de accidentes de tránsito. Características como el control electrónico de estabilidad y el frenado autónomo son ejemplos de estándares de seguridad del vehículo que pueden evitar que ocurra un choque o reducir la gravedad de las lesiones. A pesar de estos beneficios potenciales, no todos los vehículos nuevos y usados deben implementar estándares de seguridad reconocidos internacionalmente.

2.3 SEGURIDAD AUTOMOTRIZ: ISO 26262

Según (ISO 26262, 2011) Los vehículos modernos dependen en gran medida de computadoras, sensores, actuadores y redes a bordo que funcionen bien. En el sistema eléctrico y electrónico (E / E) del vehículo, la mayoría de las innovaciones futuras se llevarán a cabo ahora, cuando la industria automotriz avance rápidamente hacia un futuro con vehículos autónomos y sistemas de transporte inteligentes. Al mismo tiempo, esta área compleja también conduce a una exposición de riesgo con respecto a la seguridad funcional. ISO 26262 Seguridad funcional de vehículos de carretera es la adaptación de IEC 61508 para la industria automotriz. Define lo que se requiere para evitar un riesgo irrazonable debido a los peligros causados por el mal funcionamiento de los sistemas E / E. La implementación de ISO 26262 garantiza que se incorpore un alto nivel de seguridad en el automóvil y sus componentes desde el principio. La norma se puede utilizar para establecer un sistema de gestión de la seguridad basado en las mejores prácticas reconocidas internacionalmente y el último enfoque para la gestión de riesgos.

ISO 26262 es una norma de varias partes que define los requisitos y proporciona directrices para lograr la seguridad funcional en los sistemas eléctricos y electrónicos instalados en vehículos de carretera. La norma define un ciclo de vida de seguridad funcional que comienza con un análisis de peligros y seguridad. De este análisis se deduce el nivel de reducción de riesgo necesario para evitar un riesgo residual irrazonable y esto se define como el Nivel de Integridad de Seguridad Automotriz (ASIL).

El ASIL define las medidas de seguridad necesarias, es decir, la rigidez necesaria en el proceso al desarrollar mecanismos de seguridad a nivel de sistema, hardware y software. ASIL D representa el nivel más estricto y ASIL A el nivel menos estricto. La norma ISO 26262 también define los requisitos del sistema de gestión, la necesidad de planificación en el ciclo de vida de la seguridad funcional y los procesos de apoyo, como la gestión de requisitos, la gestión de la configuración y la gestión de cambios.

2.4 ELECTRÓNICA AUTOMOTRIZ

Basado en (Elliott, 2015) la electrónica automotriz ha controlado el latido de los automóviles desde los albores de este siglo. Desempeñan un papel clave en el diseño de las funciones del vehículo y son parte del buen funcionamiento del automóvil desde el encendido, la relación de mezcla de aire y combustible, el sistema antibloqueo de ruedas, la navegación y las complejas características de seguridad como alertas para evitar choques y frenado autónomo. La Figura 1.3 muestra diferentes Unidades de Control Electrónico (ECU) y su conexión de red.

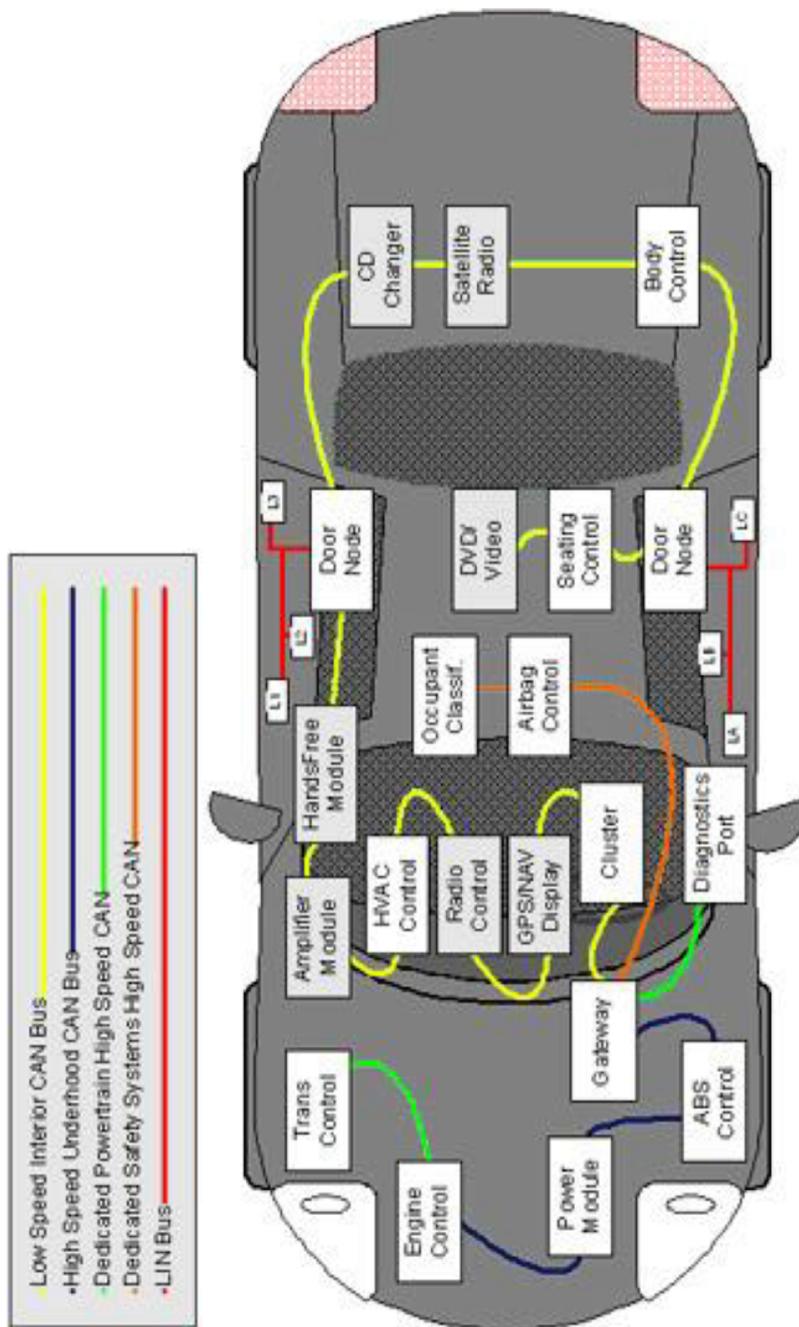


Figura 3 Diferentes ECU de un automóvil moderno, FEV (2013)

2.5 REVISIÓN BIBLIOGRÁFICA

A continuación, se detallarán las investigaciones que fueron analizadas y consultadas para el reforzamiento a la problemática planteada:

En la primera investigación consultada, (Massimo, & Gnaniah, 2019), el desarrolló en el artículo científico denominado: “Functional Safety Assessment for Advanced Driver Assistance System”, siendo el propósito de la tesis el estudiar la derivación de la seguridad funcional y del sistema requisitos para la arquitectura del Sistema avanzado de asistencia al conductor (ADAS) de el presente y el futuro.

El problema reside en las derivaciones del sistema al estar vinculado lo que producen fallas de componentes a nivel de sistema lo que provoca una falta en los requisitos de seguridad funcional y ponen en peligro al conductor. Se plantean las metodologías que se pueden utilizar (según el criterio del autor) para poder estudiar dichas fallas a fondo y poder tener un nivel de riesgo aceptable.

El enfoque metodológico utilizado se basó en el diseño presentado por ISO 26262 adoptado por el autor. Se realizó un análisis descriptivo – informativo en donde el autor se enfocó a detallar los pasos de implementación de la metodología propuesta. Al ser un estudio de tipo descriptivo, se utilizó marcos de referencias de seguridad automotriz y manuales de metodología estipulados a la fecha del año 2018. Participaron en la investigación la Facultad Ingeniería Informática de la Universidad Politécnico Di Torino en colaboración con el MCA – Engineering Di Turin.

Los resultados obtenidos brindan pautas para que los ingenieros incorporen la seguridad y la metodología del sistema durante el desarrollo de la fase conceptual del sistema.

En la segunda investigación consultada, (Carsten & Nilsson, 2001), se revisa los problemas y los procedimientos para la evaluación de seguridad del sistema de asistencia al conductor y se resalta el contraste entre las dos áreas principales del conductor. ADAS: por un lado, sistemas de información que interactúan con el conductor y por otro lado sistemas intervinientes que interactúan directamente con el vehículo.

Los sistemas de navegación son típicos de la primera categoría y el control de cruce adaptativo de la segunda. Se argumenta que, para los sistemas de información, es posible desarrollar un procedimiento de evaluación de la seguridad “genérico”, con una única prueba genérica.

Se contrasta con el ámbito de los sistemas intervinientes (sistemas de control de vehículos y de alerta al conductor), donde no es posible una evaluación genérica de este tipo mediante una única prueba. Dichos sistemas difieren ampliamente en su propósito, en su entorno operativo previsto, en su funcionalidad y en su entorno operativo.

Los resultados obtenidos se traducen en una propuesta de parte de los autores con un enfoque procedimental estructurado para la evaluación de la seguridad de los sistemas intervinientes.

En la tercera investigación consultada, (Ljung Aust, 2012) se evalúa el proceso de evaluación de las funciones de seguridad activa del sistema ADAS. El autor resalta cinco fallas empíricas que ha logrado identificar. El primer problema identificado fue la falta de un marco conceptual general para la evaluación de ADAS que pueda ayudar a formular especificaciones funcionales y generar hipótesis comprobables sobre la influencia de ADAS en escenarios críticos de conducción.

El segundo problema se refería a las formas actuales en que se utilizan los datos de accidentes para especificar escenarios de evaluación de ADAS. Se desarrolló y probó con éxito una metodología mejorada para vincular un conjunto de estudios de casos investigados en profundidad con un tipo de accidente general.

La tercera cuestión se refería a la medida en que los datos de investigaciones en profundidad de accidentes fatales se pueden utilizar para especificar escenarios de evaluación ADAS. Algunos países tienen conjuntos de datos completamente representativos investigados en profundidad para este tipo de accidentes, pero no se ha investigado su relevancia para la evaluación de ADAS. Se realizó un estudio empírico de la información de causalidad en accidentes fatales en intersecciones. Sin embargo, la información recopilada en estas investigaciones se encontró estar limitados en formas que los hacen menos útiles para definir escenarios de evaluación ADAS.

La cuarta cuestión era si los eventos de conducción suficientemente críticos que resultan en respuestas realistas del conductor se pueden crear y repetir en la evaluación ADAS basada en simuladores de conducción. Se realizó un estudio en el que dos grupos de conductores, uno con FCW y otro sin FCW, estuvieron expuestos a repetidos eventos críticos de frenado del vehículo adelantado. Los resultados indican que, si bien es posible crear un solo evento sorpresa, los efectos de interacción que comprometen la generalización del resultado se producen cuando se repite el evento crítico.

El quinto tema se refería a los principios sobre cómo evaluar la influencia combinada de múltiples ADAS cuando están presentes en el mismo vehículo. Se llevó a cabo un estudio de un paquete ADAS evaluado por FOT que consta de FCW y ACC para probar empíricamente si los modelos conceptuales existentes para calcular el efecto combinado de múltiples funciones de seguridad eran aplicables.

Los resultados indican que los modelos existentes eran demasiado simplistas para dar cuenta de las complejas modificaciones del comportamiento del conductor que se encuentran en los datos.

En la cuarta investigación, (Sini & Violante, 2020) indican que la creciente complejidad de los sistemas avanzados de asistencia al conductor (ADAS) dificulta la realización del análisis de peligros y la evaluación de riesgos (HARA).

Como resultado, implementan comportamientos complejos cuyo resultado en presencia de fallas no es trivial de identificar y clasificar según lo solicitado por la fase de concepto incluida en las normas de seguridad funcional más recientes. En este artículo se presenta una metodología basada en simulación para realizar el HARA de una función de vehículo mezclando el enfoque industrial habitual, basado en el conocimiento de los diseñadores, con uno que utiliza un simulador a nivel de vehículo. El enfoque basado en simulación proporciona un método automático y sistemático para evaluar la interacción compleja del artículo bajo análisis con otras funciones del vehículo en situaciones operativas posiblemente complejas, lo que facilita la predicción de peligros.

Se eligió demostrar el enfoque aplicándolo a un conocido caso de estudio de la industria automotriz: un sistema avanzado de frenado de emergencia (AEBS). De esta forma, es posible analizar los efectos de la función proporcionada por el ítem, teniendo en cuenta los resultados de la simulación y comparándolos con análisis de situaciones similares disponibles en la literatura. Los resultados obtenidos basados en la simulación, permitieron que los ingenieros de seguridad puedan formular una hipótesis más objetiva, en particular durante la sub fase de clasificación de peligros.

3. JUSTIFICACIÓN

El presente trabajo monográfico se enfocará en el estudio y análisis de riesgos que enfrentan los sistemas avanzados de asistencia a conductores, mejor conocidos por sus siglas en inglés (ADAS) en vehículos Volvo. El propósito de esta investigación es mediante la metodología propuesta identificar distintos tipos de riesgos asociados con la implementación y el uso de Sistemas Avanzados de Asistencia al Conductor evaluando los riesgos debido a errores de los conductores (comportamiento del conductor) y posibles desafíos de ADAS en distintas situaciones peligrosas identificadas. Tomando en cuenta los siguientes indicadores: gravedad, probabilidad de ocurrencia, detectabilidad y recuperabilidad. Para cada tipo de falla identificada, también se definirá el efecto de está, la causa, la detección, el reconocimiento y recomendaciones de objetivos de seguridad para su mitigación en la fase conceptual.

Los OEM's de la industria automotriz buscan constantemente formas de incorporar y mejorar las funcionalidades ADAS en sus vehículos. Una de las principales tareas de los fabricantes de equipos ADAS es derivar los requisitos de seguridad del sistema y asegurar su funcionalidad durante la etapa del concepto del sistema del proyecto, que se adhiere a los conceptos de ingeniería del sistema de estándares ISO 26262. Desde la década de 1990 este tipo de tecnología ha existido, pero terminaron fallando. Todas estas tecnologías del pasado ahora se están volviendo más inteligentes. Todo ha mejorado mucho en fin a reducir el potencial de lesiones para el conductor. La mayor ventaja de utilizar los sistemas de asistencia es que permiten la comunicación entre diferentes vehículos, sistemas de infraestructura de vehículos y centros de gestión de transporte. Esto permite el intercambio de información para una mejor visión, localización, planificación y toma de decisiones de los vehículos.

4. OBJETIVOS

OBJETIVO GENERAL

Desarrollar un análisis de seguridad y asesoramiento de riesgos del sistema avanzado de asistencia a conductores en los vehículos Volvo para identificar los distintos tipos de escenarios y fallas asociados con la intervención humano - interfaz durante la operatividad del sistema.

OBJETIVOS ESPECÍFICOS

1. Evaluar el impacto relativo y efectos de diferentes fallas y/o riesgos provocados por el comportamiento del conductor o el interfaz mediante un análisis FMEA.
2. Identificar el mal funcionamiento que podría conducir a escenarios peligrosos y evaluar el riesgo de estos, mediante el desarrollo de un análisis HARA del sistema ADAS.
3. Determinar un objetivo de seguridad para cada evento peligroso evaluado correspondiente al nivel de riesgo, ASIL. Los objetivos de seguridad son requisitos de seguridad funcional de alto nivel como resultado del análisis de peligros y la evaluación de riesgos.

5. MARCO TEÓRICO

En el presente capítulo se establece la base conceptual de la investigación donde se presentan los conceptos y definiciones de los componentes, funciones, sensores, los niveles de automatización, así como el marco de referencia relacionado al ciclo de vida y seguridad automotriz respecto a ISO 26262, además se incorpora la metodología propuesta por el estándar utilizado posteriormente como marco de referencia en el desarrollo del análisis de seguridad. Igualmente, las cláusulas del estándar con mayor relevancia para esta investigación.

5.1 DEFINICIÓN DEL SISTEMA ADAS

(Shaout, Colella & Awad, 2011) Indica que los profesionales de la seguridad entienden ADAS como sistemas de seguridad inteligentes basados en vehículos que podrían mejorar la seguridad vial en términos de prevención de choques, mitigación y protección de la gravedad de los choques y notificación automática de colisión anterior al choque; o incluso sistemas integrados en el vehículo o basados en infraestructura que contribuyen a algunas o todas estas fases de la colisión. De manera más general, algunos sistemas de apoyo al conductor están destinados a mejorar la seguridad, mientras que otros son funciones de conveniencia para el conductor.

El ADAS actual combina una serie de tecnologías para operar. En esencia, cada sistema comprende al menos un sensor para monitorear parámetros dados y transmitir cuando sea necesario información que luego se procesa y analiza antes, si es necesario, enviar un comando para dar una alerta sensorial al conductor o para intervenir y ayudar con el control del vehículo. Con algunos sistemas, y bajo ciertas condiciones, puede ocurrir una combinación de algunos de los mencionados a continuación.

5.2 COMPONENTES DE ADAS

5.2.1 SISTEMA ANTIBLOQUEO DE FRENOS

(Jitesh, 2014) Define a los componentes básicos del ABS, los cuales son sensores de velocidad de las ruedas, válvulas conmutables en las líneas hidráulicas, una bomba y un módulo de control electrónico. El sistema funciona monitoreando las velocidades de las ruedas y detectando la desaceleración rápida de las ruedas inmediatamente antes de un bloqueo, luego reduce brevemente y luego vuelve a aplicar la presión hidráulica en una acción pulsante.

Imita la acción de frenado con cadencia de bombeo del pedal que una vez se enseñó a los conductores como técnicas para evitar derrapes a una frecuencia mucho más alta, alrededor de 15/20 veces por segundo en los sistemas actuales.

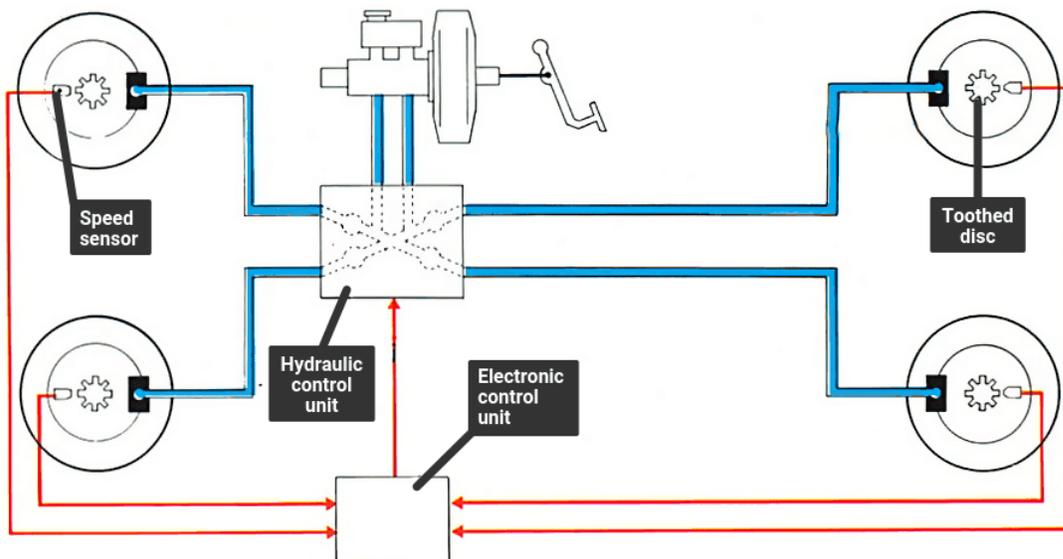


Figura 4 Diagrama de funcionalidad de ABS, Jitesh (2014)

5.2.2 CONTROL DE ESTABILIDAD ELECTRÓNICO

(NHTSA, 2020) El control electrónico de estabilidad (ESC) monitorea la estabilidad del vehículo e interviene para mantener el control cuando se predice una anomalía direccional probable que parezca contraria a las entradas del conductor. Las intervenciones suelen tener lugar al tomar una curva, ya sea debido a una velocidad de entrada excesiva o entradas de control erróneas, y durante maniobras evasivas o cambios de dirección repentinos. Al combinar el hardware del ABS con un sensor de posición del volante, un sensor de velocidad de guiñada y un sensor de aceleración lateral.

El ESC puede comparar los movimientos del vehículo con las presuntas intenciones del conductor para evitar una pérdida de control que, de otro modo, podría provocar que el vehículo abandone la carretera y posiblemente se vuelque. Esencialmente, el sistema funciona frenando momentáneamente las ruedas individuales para ofrecer una reacción de torsión alrededor del eje vertical contraria al movimiento involuntario del vehículo.

En algunos casos, y con algunos sistemas, el ESC también puede reducir el par del motor, mediante el retardo del encendido, el control del suministro de combustible, la supresión de chispas o la activación directa del acelerador, para mitigar aún más la pérdida de control prevista. La mayor parte del tiempo la intervención del ESC es muy sutil o incluso pasa desapercibida para el conductor, pero su eficacia para reducir accidentes, lesiones y muertes es universalmente reconocida.

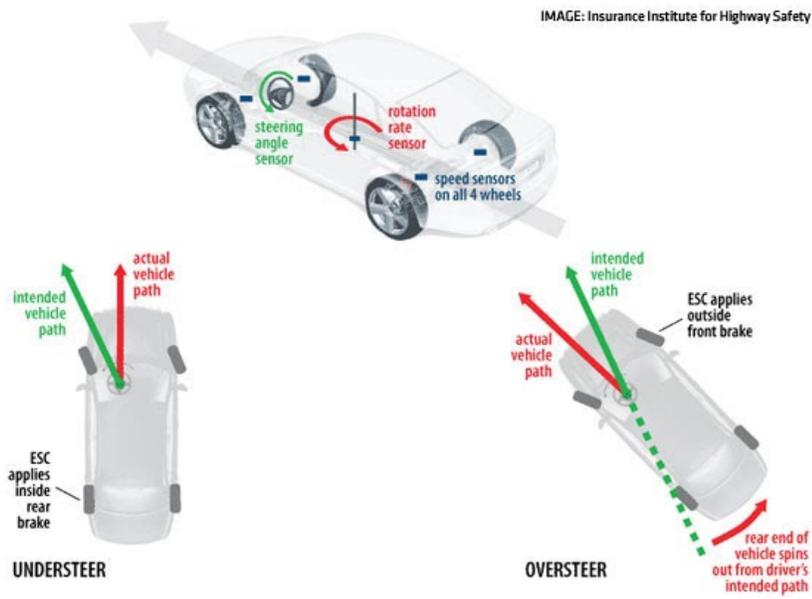


Figura 5 Funcionalidad del control electrónico de estabilidad, NHTSA (2020)

5.2.3 SISTEMA DE CONTROL DE TRACCIÓN

(ISO 7000:2045, 2004) Es esencialmente una función subsidiaria de ESC. El sistema de control de tracción es básicamente lo opuesto al ABS: sí una rueda motriz gira demasiado rápido al acelerar. En el caso de un exceso de la velocidad medida en la carretera, se suprimirá el par de esa rueda hasta que se recupere la tracción.

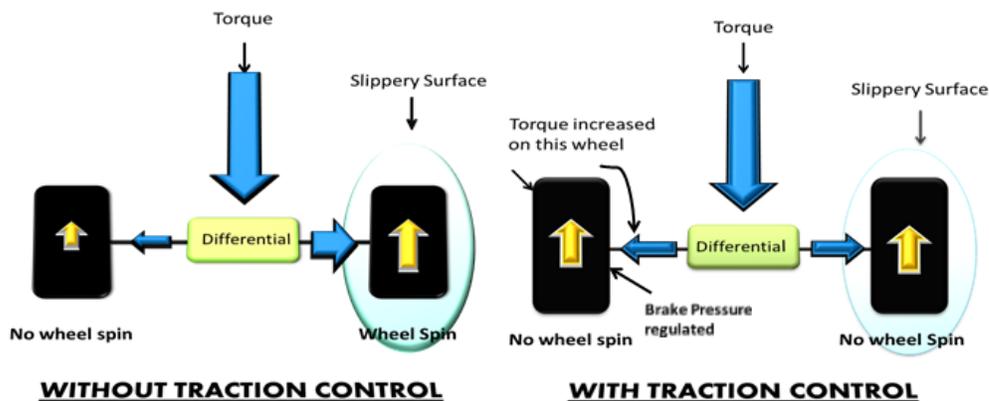


Figura 6 Funcionalidad del sistema de control de tracción, ISO 7000:2045 (2004)

5.2.4 CONTROL DE CRUCERO Y CONTROL ADAPTATIVO

(Pananurak et al., 2009) En su forma básica, el control de cruceo es un dispositivo electrónico en un vehículo que controla el acelerador para mantener una velocidad constante. El conductor enciende la función para hacer que el vehículo continúe a la velocidad que haya elegido.

El control de cruceo adaptativo (ACC) es una forma inteligente de control de cruceo que ralentiza y acelera automáticamente para seguir el ritmo del automóvil que tiene delante. El conductor establece la velocidad máxima, al igual que con el control de cruceo, luego un sensor de radar observa el tráfico de adelante, se fija en el automóvil en un carril e indica al automóvil que se quede unos segundos detrás del automóvil de la persona que va delante (el conductor establece la distancia).

El ACC ahora casi siempre está emparejado con un sistema previo al choque que lo alerta y, a menudo, comienza a frenar. El control de cruceo adaptativo también se denomina control de cruceo activo, control de cruceo autónomo, control de cruceo inteligente o control de cruceo por radar. Este es el caso porque la distancia se mide con una pequeña unidad de radar detrás de la rejilla delantera o debajo del parachoques. Algunas unidades emplean un láser, mientras que otras usan un sistema óptico basado en cámaras estereoscópicas.

Independientemente de la tecnología, ACC funciona día y noche, pero sus capacidades se ven obstaculizadas por la lluvia intensa, la niebla o la nieve. El ACC es una parte fundamental de los vehículos autónomos del futuro cercano. En un automóvil de conducción autónoma, ACC necesita rastrear el automóvil que está delante, pero también los automóviles en carriles adyacentes en caso de que sea necesario un cambio de carril.

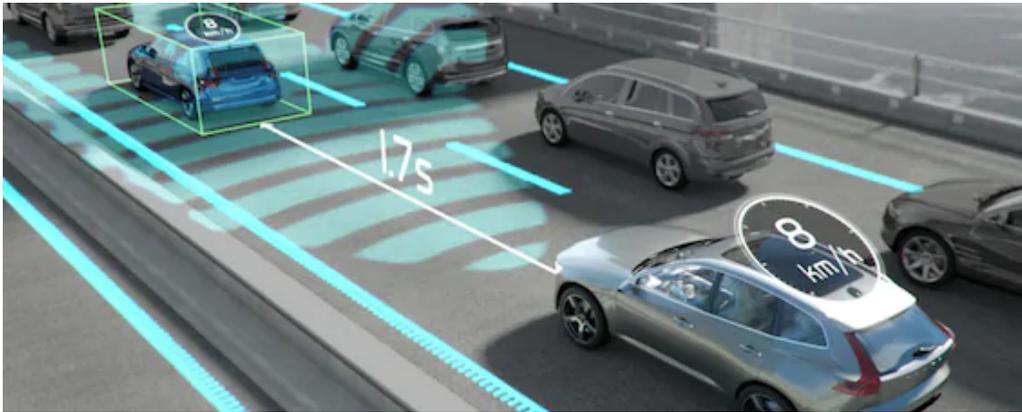


Figura 7 Control de Crucero en Vehículos Volvo, Volvo Cars AB (2018)

5.2.5 AVISO DE COLISIÓN FRONTAL Y FRENADO DE EMERGENCIA AUTÓNOMA

(Zador et al., 2000) Aviso de Colisión Frontal (FCW) es un sistema que informa al conductor a través de una alerta visual y / o táctil que es necesario frenar para evitar que ocurra una colisión. Los sistemas de solo FCW no tienen Frenado de Emergencia Autónoma (AEB) instalado para ayudar con el frenado. En un automóvil equipado con AEB, se dará la alerta FCW visual y / o táctil, seguida de que el vehículo aplique automáticamente los frenos de una manera predeterminada y calculada para evitar o reducir la velocidad de colisión.

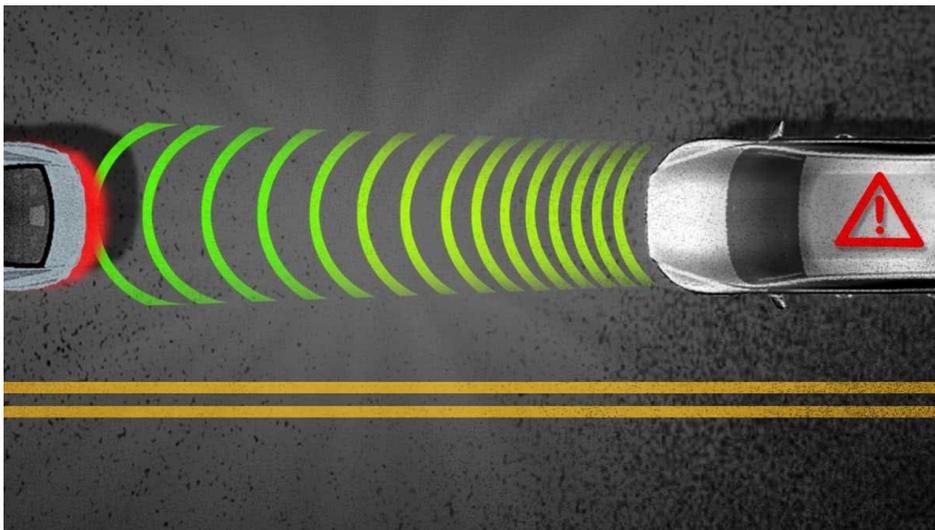


Figura 8 Advertencia de colisión frontal, Volvo Cars AB (2014)

AEB y FCW suelen utilizar un módulo de control común. Dependiendo del proveedor, el módulo para procesar los sensores de proximidad y radar son independientes del módulo de control de frenos / ABS. FCW y AEB pueden usar una variedad de sensores diferentes para determinar la distancia, la velocidad y la aceleración entre el automóvil y un automóvil u objeto que se encuentre adelante.



Figura 9 Frenado de Emergencia Autónomo, Volvo Cars AB (2018)

5.2.6 SUPERVISIÓN DE PUNTOS CIEGOS / ASISTENCIA DE CAMBIO DE CARRIL

(NHTSA, 2014) indica que el monitoreo de puntos ciegos utiliza un conjunto de sensores montados en los espejos laterales o en el parachoques trasero para detectar vehículos en los carriles adyacentes. Si los sensores detectan algo, lo alertarán mediante una advertencia audible y / o visual. Algunos vehículos utilizan una cámara como parte principal del sistema o para complementar los sensores. La actualización reciente al monitoreo de punto ciego es un cambio de advertencia pasiva a ayudar activamente al conductor a evitar una posible colisión.

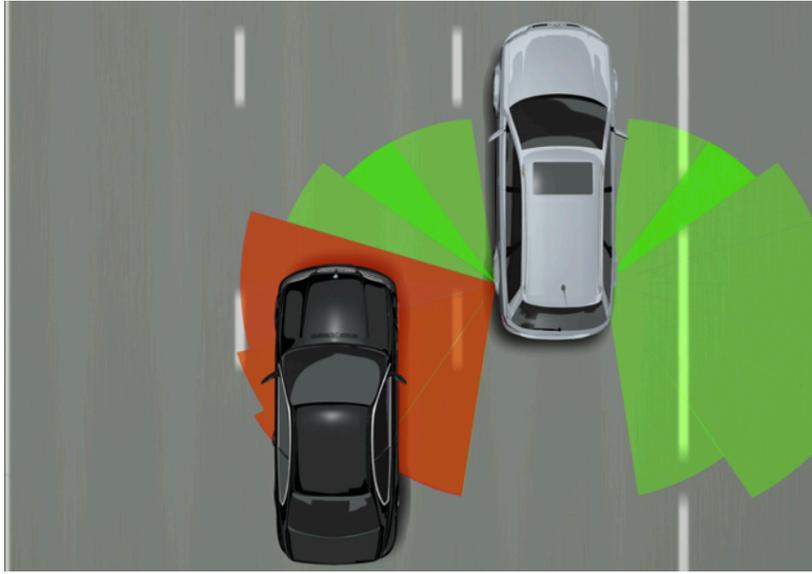


Figura 10 Sistema de asistencia a la decisión de cambio de carril, Volvo Cars AB (2014)

5.2.7 AVISO DE SALIDA DE CARRIL / AYUDA DE MANTENIMIENTO DE CARRIL

(Hoover et al., 2014) La asistencia para mantenerse en el carril y la advertencia de cambio de carril son términos de la industria para la tecnología que se enfoca en evitar que un automóvil se salga de su carril. Los sistemas de advertencia de cambio de carril simplemente alertan al conductor cuando el automóvil está saliendo de su carril, mientras que la asistencia para mantenerse en el carril realmente funciona para evitar que el automóvil se salga del carril.

Los sistemas de advertencia de cambio de carril escanean la carretera para determinar dónde están las líneas límites del carril. Si el automóvil pasa por encima de estos marcadores, el sistema se lo permite al conductor, generalmente emitiendo un pitido o mostrando un mensaje de advertencia en el tablero. Luego, es el conductor quien debe tomar medidas correctivas. La asistencia para mantenerse en el carril lleva las cosas un paso más allá al permitir que el automóvil se dirija en la dirección correcta.

La cantidad de entrada de dirección puede variar desde suaves empujones destinados a guiar al conductor hasta intervenciones completas. Debido a que las capacidades de esta tecnología varían de un sistema a otro, es importante conocer las limitaciones del automóvil en particular antes de ceder las tareas de mantenimiento de carril a las máquinas.



Figura 11 Sistema Volvo de advertencia de cambio de carril, Volvo Cars AB (2018)

5.2.8 SENSOR DE ESTACIONAMIENTO / SISTEMA DE ASISTENCIA DE ESTACIONAMIENTO

Según (Shimizu & Sako, 2000) el asistente de estacionamiento, se refiere a un asistente de estacionamiento automatizado que utiliza tecnología de radar, cámaras y sensores. Permite que el automóvil haga la mayor parte del trabajo por sí mismo cuando se estaciona en un lugar ubicado en un estacionamiento o al costado de la carretera. Los sensores a bordo del automóvil comenzarán a buscar espacios de estacionamiento adecuados.

Cuando detecta un espacio de estacionamiento potencial cercano, los sensores lo analizarán y determinarán si el espacio es de un tamaño razonable y si el automóvil se puede maniobrar en él. Una lectura confirmará al conductor si considera que el lugar de estacionamiento cercano es adecuado. El asistente de aparcamiento le mostrará el camino inverso previsto a través de una pantalla multifuncional a bordo. Luego, comenzará a girar automáticamente hacia el lugar de estacionamiento mientras retrocede hacia él.



Figura 12 Detección de puntos del sistema de asistencia de estacionamiento, Volvo Cars AB (2018)

5.2.9 ALERTA DE TRÁFICO CRUZADO

(Auto Vision News, 2020) Indica que, Alerta de Tráfico Cruzado (CTA) es un apoyo al conductor complementario destinado a ayudar al conductor a detectar el tráfico que se cruza detrás del automóvil cuando se da marcha atrás.

La subfunción de freno automático puede detener el automóvil si existe riesgo de colisión con un vehículo no observado.

CTA complementa la información de puntos ciegos al poder ver el tráfico que se cruza desde un lado. El CTA está diseñado para detectar vehículos principalmente; en casos favorables, incluso se pueden detectar objetos más pequeños como bicicletas y peatones.

CTA solo está activo si el automóvil rueda hacia atrás o si se selecciona la posición de marcha atrás de la caja de cambios. Si el conductor no presta atención a la advertencia de la CTA y una colisión es inevitable, la función de freno automático entra para detener el automóvil y la pantalla del conductor muestra un mensaje de texto explicativo de por qué se frenó el automóvil.

La función es una ayuda adicional para el conductor con la intención de facilitar la conducción y hacerla más segura; sin embargo, no puede manejar todas las situaciones en todas las condiciones de tráfico, clima y carretera.



Figura 13 Icono de CTA en el gráfico de asistencia de estacionamiento del monitor. Volvo Cars AB (2020)

5.2.10 ASISTENCIA DE GIRO

(NEOPLAN, 2020) Menciona que el asistente de giro es un nuevo sistema avanzado de asistencia al conductor introducido en 2015. El sistema monitorea el tráfico opuesto al girar a la izquierda a baja velocidad.

En situaciones críticas, frena el coche. Este es un escenario común en los cruces de ciudades con mucho tráfico, así como en las carreteras, donde los límites de velocidad son más altos.

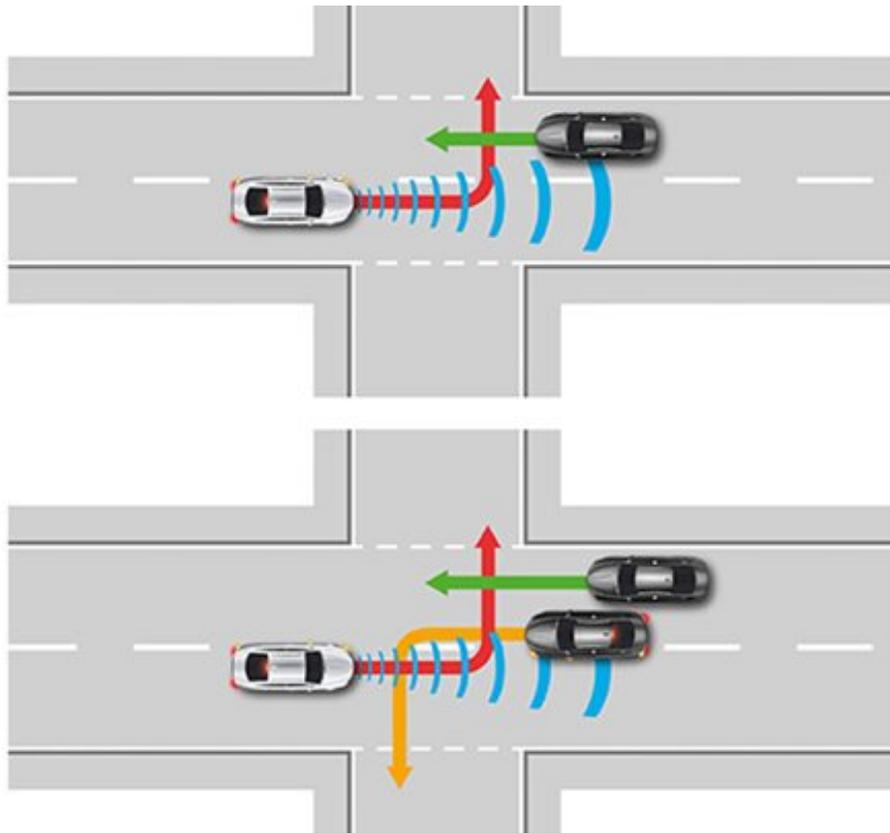


Figura 14 Sistema de Asistencia de Giro, NEOPLAN (2020)

5.2.11 GLARE - FREE HIGH BEAM

(K.R.K. Sastry, 2015) “Glare free high beam” es una estrategia de control de iluminación dinámica impulsada por una cámara que sombrea de forma selectiva los puntos y corta el patrón de luz de carretera para proteger a otros usuarios de la carretera del deslumbramiento, simultáneamente proporciona al conductor el máximo rango de visión. El área que rodea a otros usuarios de la carretera está constantemente iluminada con una intensidad de luz alta, pero sin el deslumbramiento que normalmente resultaría del uso de luces altas no controladas en el tráfico.

Este patrón de haz que cambia constantemente requiere sensores, microprocesadores y actuadores complejos porque los vehículos que deben estar a la sombra del haz se mueven constantemente. El sombreado dinámico se puede lograr con máscaras de sombra móviles desplazadas dentro de la trayectoria de la luz dentro del faro. O bien, el efecto se puede lograr oscureciendo selectivamente los emisores LED direccionales o los elementos reflectores, una técnica conocida como luz de píxel.

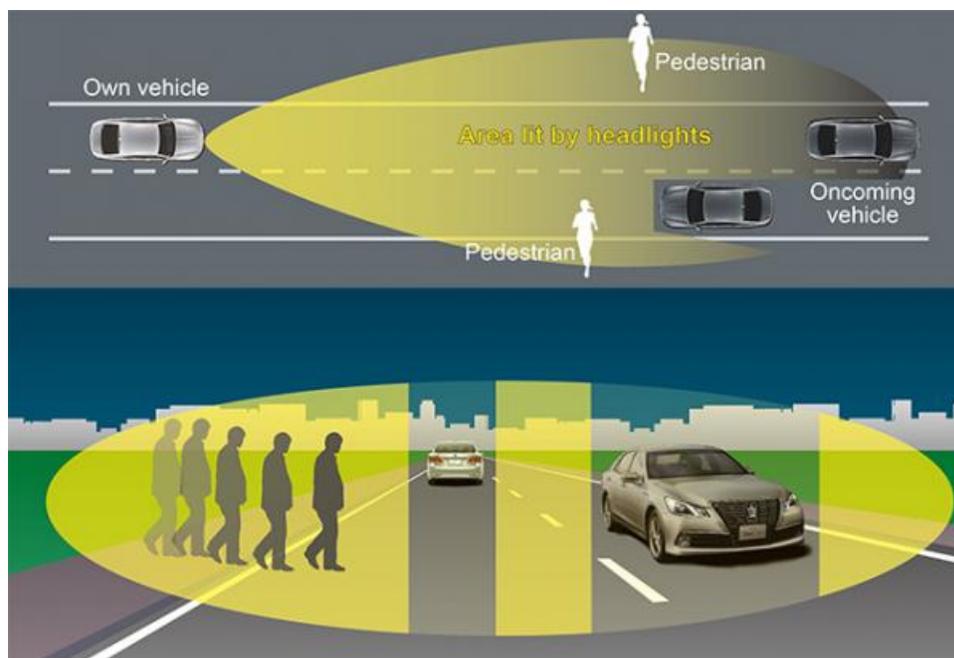


Figura 15 Sistema Glare - free High Beam, Bosch (2017)

5.2.12 SISTEMA DE NAVEGACIÓN AUTOMOTRIZ

(Skog & Händel, 2009) Un sistema de navegación automotriz es parte de los controles del automóvil o un complemento de terceros que se utiliza para encontrar la dirección en un automóvil. Por lo general, utiliza un dispositivo de navegación por satélite para obtener sus datos de posición que luego se correlacionan con la posición respecto a la carretera. Cuando se necesitan direcciones, se puede calcular la ruta. La información de tráfico sobre la marcha se puede utilizar para ajustar la ruta. Para una mayor confiabilidad, se puede utilizar un giroscopio y un acelerómetro utilizando los datos de distancia de los sensores conectados al tren motriz, ya que la pérdida de la señal del GPS y / o la trayectoria múltiple pueden ocurrir debido a interferencia o túneles urbanos.

Matemáticamente, la navegación automotriz se basa en el problema del camino más corto, dentro de la teoría de grafos, que examina cómo identificar el camino que mejor cumple con algunos criterios (más corto, más barato, más rápido, etc.) entre dos puntos en una red grande. Los sistemas de navegación para automóviles son cruciales para el desarrollo de automóviles autónomos.



Figura 16 Sistema de Navegación GPS de Vehículos Volvo, Volvo Cars AB (2020)

5.2.13 VISIÓN NOCTURNA AUTOMOTRIZ

(Mollick, 2010) Los casos de uso de la función de visión nocturna son en su mayoría caminos rurales no iluminados y situaciones con vehículos que se acercan y que pueden ocultar a peatones, ciclistas o cualquier obstáculo en el propio carril debido al deslumbramiento.

Independientemente de sus tecnologías básicas, el principio de esta función es presentar una imagen en vivo mejorada en tiempo real en las proximidades del campo primario de visión del conductor. Hay dos variantes de técnicas de sistemas de mejora de la visión nocturna en el mercado:

- Sistema de infrarrojo lejano (FIR) Los sistemas de mejora de la visión nocturna FIR reciben radiación térmica emitida por objetos en el rango de longitud de onda del infrarrojo lejano entre 7 y 12 μm . Estos llamados sistemas pasivos no requieren ninguna fuente adicional de radiación para iluminar los objetos. La imagen de la cámara puede ser procesada por una ECU para mejorar la calidad de la imagen y luego es presentada por una pantalla gráfica al conductor.
- Sistema de infrarrojo cercano (NIR) Los sistemas de infrarrojo cercano utilizan radiación en el rango espectral entre 800 nm y 1000 nm. Dado que los objetos no emiten ninguna radiación en este rango de longitudes de onda, los objetos que se encuentran frente al vehículo deben estar iluminados. Los reflejos son recogidos por una cámara de video sensible a infrarrojos.

5.2.14 ESTABILIZACIÓN DE VIENTO CRUZADO

(Duke Science & Society, 2018) La estabilización del viento cruzado permite que el vehículo compense los vientos cruzados frenando. El sistema detecta ráfagas de viento laterales a través de sensores que monitorean el movimiento de rotación de las ruedas y contrarrestan su fuerza aplicando frenos en las ruedas del lado que experimenta el viento.

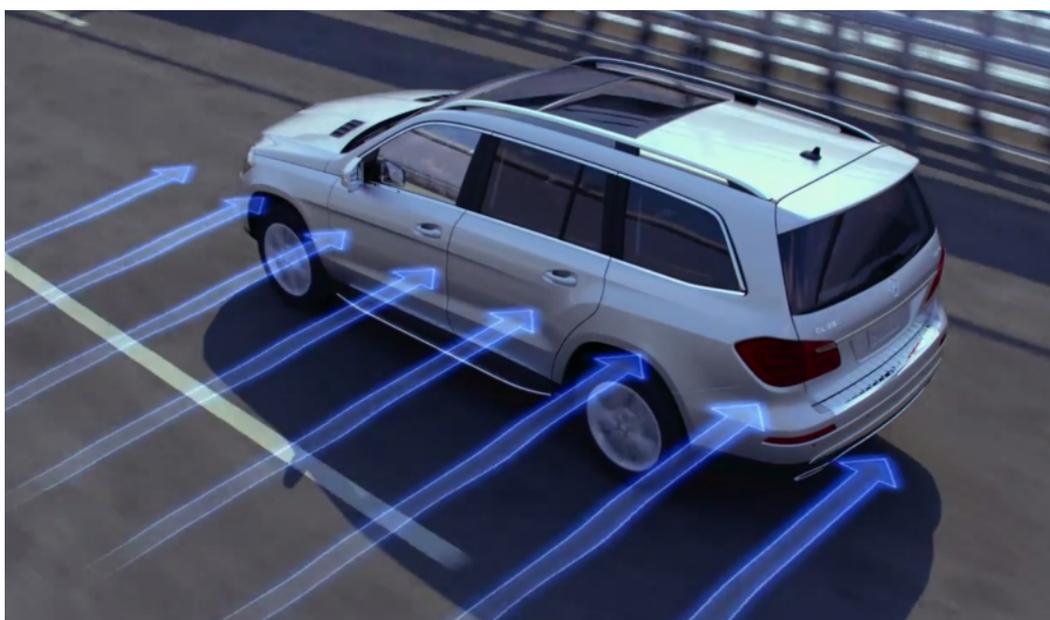


Figura 17 Estabilización de Viento Cruzado, Damler (2014)

5.2.15 ADAPTACIÓN DE VELOCIDAD INTELIGENTE (ISA)

(EU Commission for Mobility & Transport, 2016) La Adaptación Inteligente de Velocidad (ISA) es un sistema en el vehículo que usa información sobre la posición del vehículo en una red en relación con el límite de velocidad vigente en esa ubicación en particular. ISA puede ayudar a los conductores a cumplir con el límite de velocidad en cualquier lugar de la red. Esta es una ventaja importante en comparación con los limitadores de velocidad para vehículos pesados y autocares, que solo limitan la velocidad máxima.

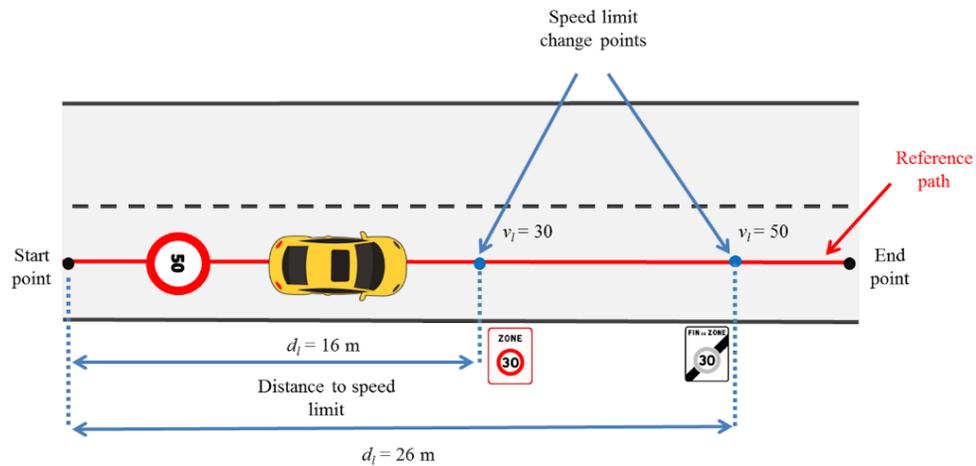


Figura 18 Adaptación de Velocidad Inteligente, EU Commission for Mobility & Transport (2016)

5.2.16 SURROUND VIEW SYSTEM

La vista envolvente automotriz, también llamada "vista alrededor" o "sistema de monitoreo de visión envolvente", es una tecnología ADAS automotriz emergente que brinda al conductor una vista de 360 grados del área que rodea el vehículo. Los sistemas de visión envolvente normalmente constan de cuatro a seis cámaras de ojo de pez montadas alrededor del vehículo, por ejemplo, una en el parachoques delantero, otra en el parachoques trasero y una debajo de cada espejo lateral.



Figura 19 Surround View System, Volvo Cars AB (2020)

5.2.17 SISTEMA DE CONTROL DE PRESIÓN DE NEUMÁTICOS

Los sistemas de control de la presión de los neumáticos se pueden dividir en dos categorías: sistemas indirectos y directos. Los sistemas indirectos miden las revoluciones por minuto de los neumáticos y en caso de cualquier desviación, el sistema envía la indicación. En los sistemas directos, la presión dentro de cada neumático se detecta mediante sensores de presión.



Figura 20 Alerta de Presión de Neumáticos, Volvo Cars AB (2017)

5.2.18 SISTEMA DE MONITOREO DEL CONDUCTOR

(Veoneer, 2019) Los sistemas de monitoreo del conductor (DMS) pueden invocar acciones para mantener la atención del conductor tanto en situaciones de conducción manual como autónoma. El DMS puede detectar conductores distraídos y somnolientos midiendo con precisión la posición de los ojos, la cabeza, la atención y la fatiga del conductor. El DMS invocará la acción cuando se detecte una situación peligrosa o sea inminente. Un análisis confiable del estado del conductor también permitirá desarrollar tecnologías que son críticas para respaldar funciones de conducción altamente autónomas, con un funcionamiento seguro sin manos al volante.

El DMS comprende el comportamiento del conductor, lo que permite que los vehículos del mañana tomen mejores decisiones para mejorar la comodidad y la seguridad.

La detección de somnolencia del conductor es una tecnología de seguridad del automóvil que ayuda a prevenir accidentes causados por la somnolencia del conductor. Varios estudios han sugerido que alrededor del 20% de todos los accidentes de tráfico están relacionados con la fatiga, hasta un 50% en determinadas carreteras



Figura 21 Detección de Somnolencia del Conductor, Bosch (2018)

5.2.19 SISTEMA DE SONIDO DE ADVERTENCIA DE VEHÍCULOS ELÉCTRICOS

(Pellkofer et al., 2020) Los vehículos tradicionales con motor de combustión emiten sonido de motor, incluso a bajas velocidades de desplazamiento. Por lo general, los peatones y otros participantes del tráfico reconocen un vehículo que se acerca o sale a través de la identificación visual y auditiva de los sonidos de las llantas y otros ruidos emitidos cuando el vehículo está fuera de la vista. Los vehículos eléctricos (EV) no emiten sonido de motor.

Los vehículos eléctricos híbridos (HEV) o los vehículos eléctricos híbridos enchufables (PHEV) se mueven casi en silencio cuando viajan a bajas velocidades antes de que se active el motor de combustión interna convencional (ICE). Estos vehículos son difíciles de escuchar cuando se viaja a velocidades inferiores a 19 mph. A mayores velocidades, el sonido de los neumáticos se vuelve dominante.

Los órganos de gobierno mundiales están explorando una legislación que busca establecer un nivel mínimo de sonido para los PHEV y HEV cuando operan en modo eléctrico, de modo que las personas con discapacidad visual, los peatones y los ciclistas puedan escuchar estos vehículos acercarse y determinar desde qué dirección se están acercando. Un sistema de sonido de advertencia de vehículos eléctricos (AVAS) produce una serie de sonidos diseñados para alertar a los peatones sobre la presencia de EV, HEV y PHEV. El conductor puede iniciar sonidos de advertencia (similar al sonido de la bocina de un automóvil, pero menos urgente); sin embargo, los sonidos deben habilitarse automáticamente a bajas velocidades. Estos sonidos varían desde tonos artificiales hasta sonidos realistas que imitan el ruido del motor y los neumáticos que se mueven sobre la grava.

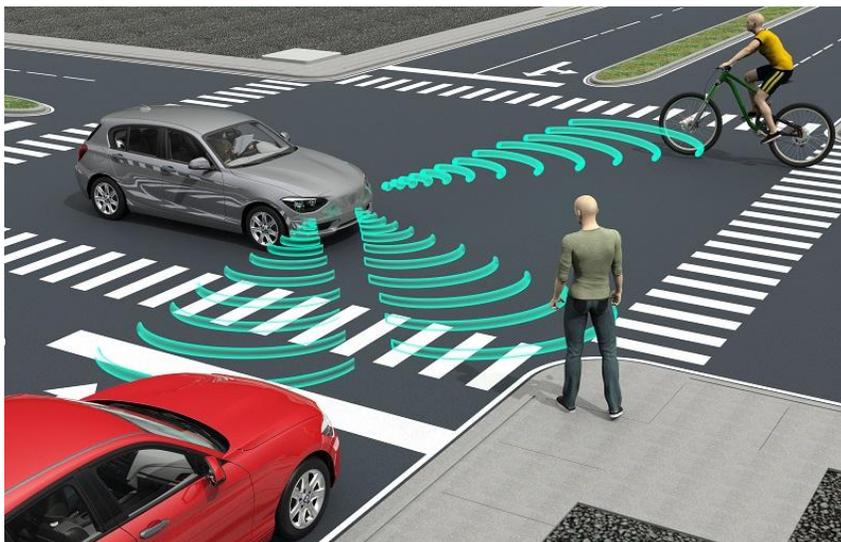


Figura 22 Sistema Acústico de Advertencia, Bosch (2018)

5.2.20 CONTROL DE DESCENSO EN PENDIENTES

(Volvo Cars, 2016) El Control de descenso de pendientes (HDC) permite aumentar / disminuir la velocidad en descensos empinados, con el pie en el pedal del acelerador únicamente, sin usar el freno de servicio.

La sensibilidad del pedal del acelerador se vuelve más pequeña y más precisa porque el control completo del pedal solo puede regular la velocidad del motor dentro de un rango de velocidad limitado.

El sistema de frenos opera solo y le da al automóvil una velocidad baja y uniforme, por lo que el conductor puede concentrarse completamente en la dirección. El HDC es especialmente útil en pendientes pronunciadas con terreno irregular y secciones resbaladizas. Por ejemplo. Al botar un bote en un remolque desde una rampa.

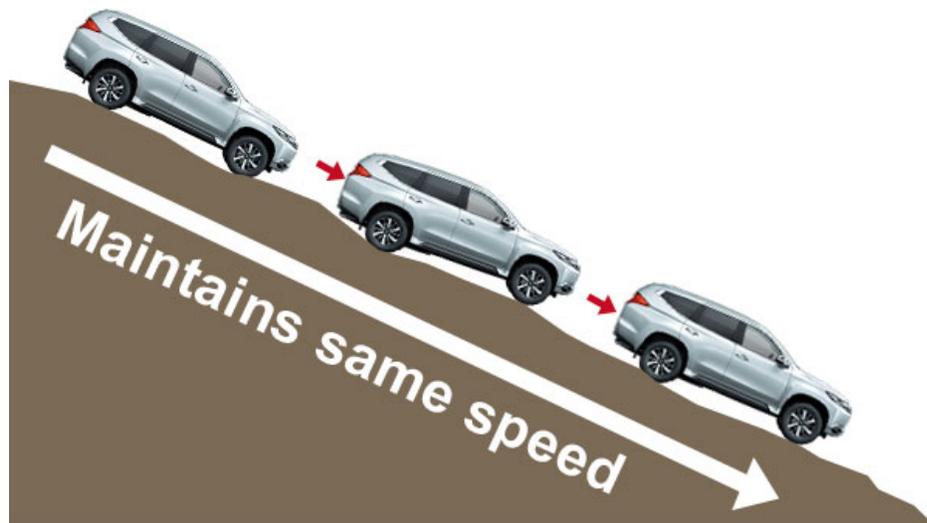


Figura 23 Control de Descenso en Pendientes, Volvo Cars AB (2015)

5.2.21 RECONOCIMIENTO DE SEÑALES DE TRÁFICO

(Fleyeh, 2008) El reconocimiento de señales de tráfico (TSR) es una tecnología mediante la cual un vehículo puede reconocer las señales de tráfico colocadas en la carretera, como, "límites de velocidad" o "niños" o "girar hacia adelante".

Utiliza técnicas de procesamiento de imágenes para detectar las señales de tráfico. Los métodos de detección se pueden dividir generalmente en métodos basados en colores, basados en formas y basados en aprendizaje.



Figura 24 Reconocimiento de Señales de Tráfico, Volvo Cars AB (2016)

5.3 SENSORES DE ADAS

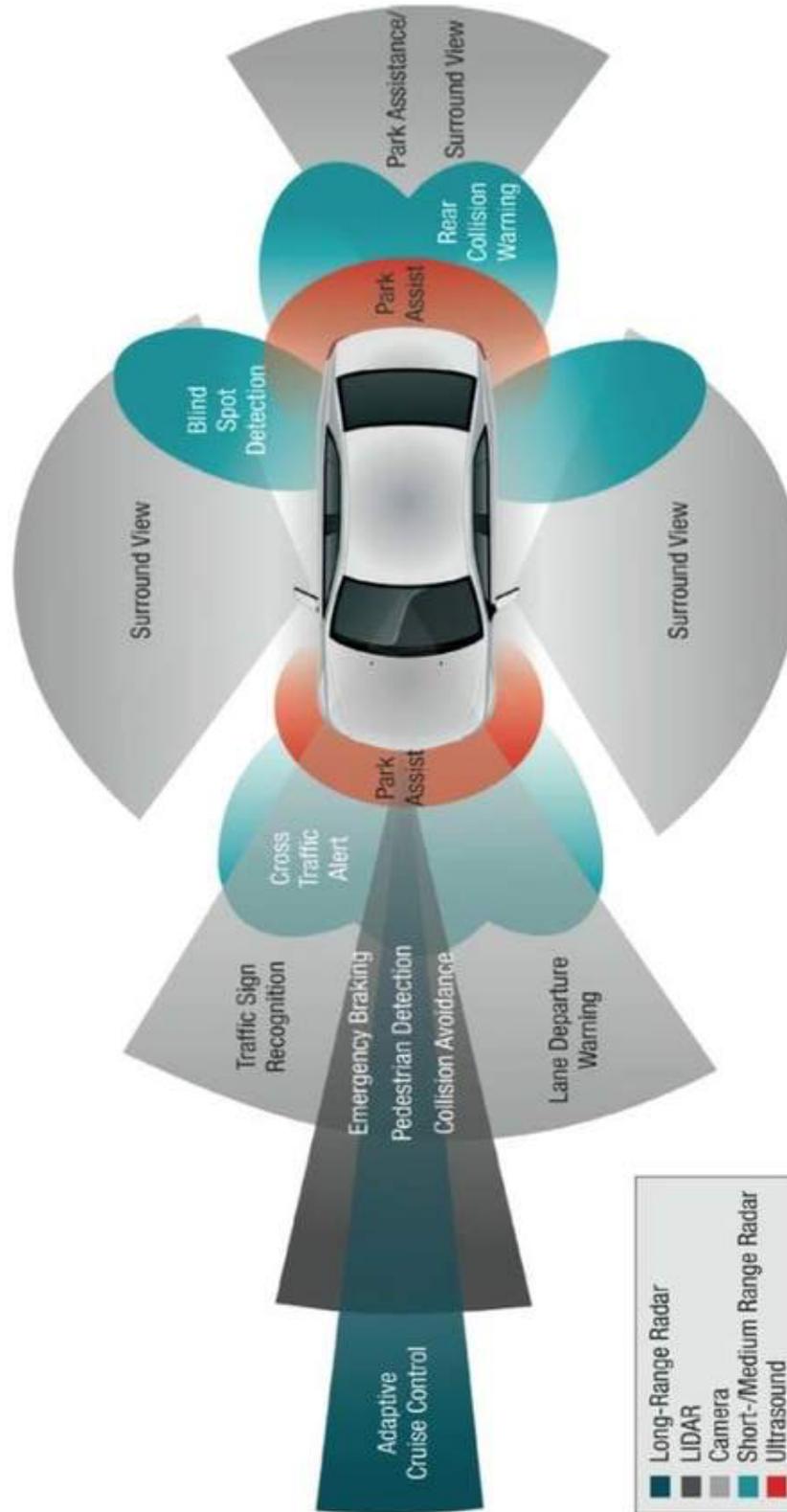


Figura 25 Funciones y sensores ADAS, SAE (2016)

5.3.1 RADAR

5.3.1.1 Principio de Funcionamiento

(Parker, 2017) La técnica, denominada RADAR (Radio Detection And Ranging), funciona según el principio de una fuente que transmite la onda de radio, es reflejado por una superficie y recibido y procesado por un sistema receptor.

De manera más simple, un sistema de radar generalmente consta de los siguientes subsistemas:

- Transmisor: Las señales alimentadas por amplificador se generan aquí utilizando un generador de forma de onda.
- Guías de ondas: como sugieren los nombres, facilitaron la transmisión de señales de radar.
- Antena: transfiere la energía del transmisor a señales en el espacio.
- Receptor: Se utiliza para la detección y captura de señales.
- Unidad de procesamiento: utiliza señales capturadas y sus propiedades para derivar la detección, el alcance y otra información útil.

El radar automotriz generalmente funciona en 77 GHz y se divide en tres categorías:

1. Radar de corto alcance (SRR): de 0,5 a 20 metros
2. Radar de alcance medio (MRR): 1 a 60 metros
3. Radar de largo alcance (LRR): de 10 a 250 metros

5.3.1.2 Funcionamiento de Características

RADAR habilita las siguientes características:

- Detección general de objetos
- Monitoreo de punto ciego
- Advertencia de colisión
- Asistente de estacionamiento
- Frenado de emergencia automático

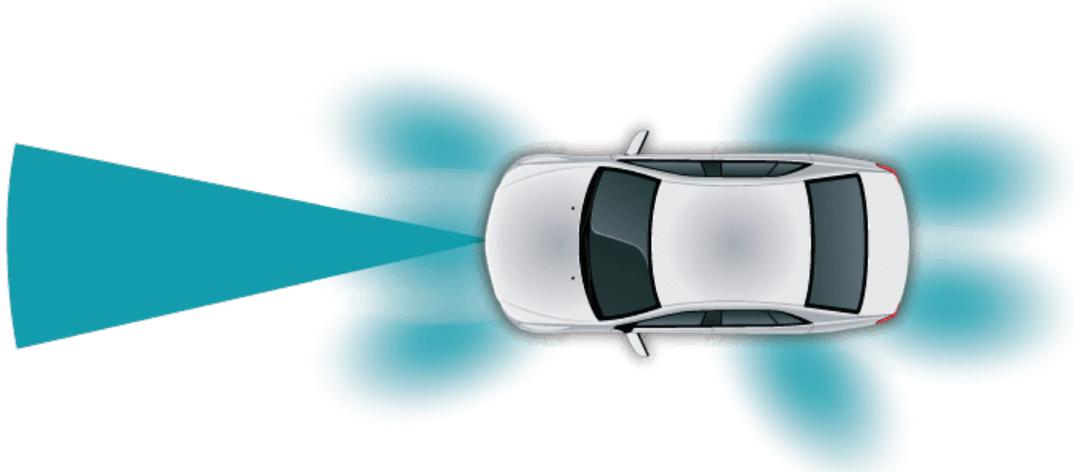


Figura 26 Fusión del sistema de radar en ADAS, Texas Instruments (2018)

5.3.2 SENSOR DE VIDEO

(ZMP, 2013) Explica que los sistemas avanzados de asistencia al conductor (ADAS) que utilizan sensores basados en cámaras ayudan al conductor y al vehículo a tener una mayor conciencia del entorno de conducción.

Las cámaras se colocan fuera del vehículo en la parte delantera, trasera y laterales para capturar imágenes de la carretera, señales de tráfico, peatones, vehículos y otros obstáculos. Las imágenes capturadas por las cámaras se analizan mediante un software de apoyo y la información desencadena una respuesta para mejorar la seguridad.

Esto podría ser iniciar automáticamente el frenado de emergencia, alertar al conductor de que se está saliendo de un carril o que hay un vehículo en su punto ciego, o ayudarlo a estacionar el automóvil.

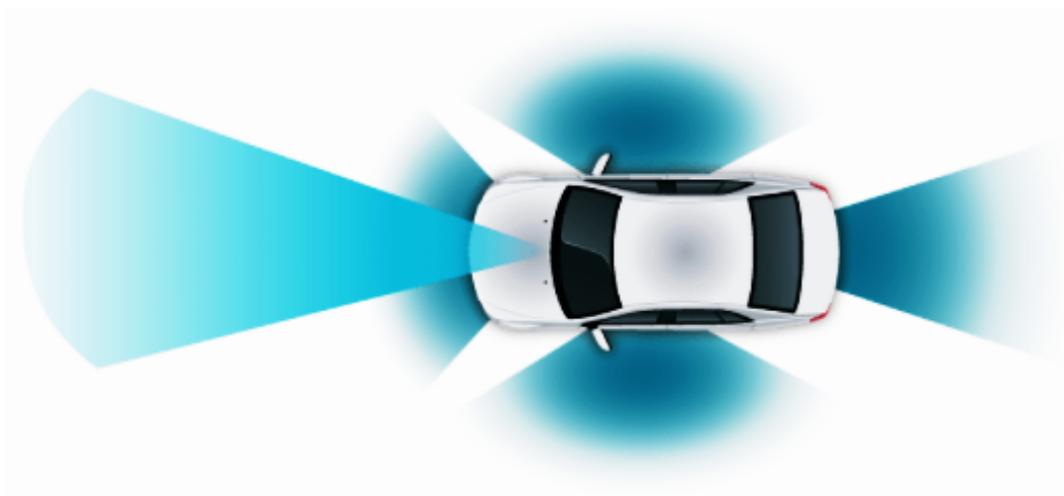


Figura 27 Fusión del sistema de cámara en ADAS, Texas Instruments (2018)

5.3.2.1 Tipos

Sistema de Visión Mono

(Munster, 2018) El sistema de visión única está compuesto por hardware y algoritmos totalmente integrados que identifican objetos como automóviles, marcas o señales viales. El procesador puede activar alarmas, mostrar información gráfica al conductor y detener automáticamente el vehículo.

Los sistemas de visión mono habilitan las siguientes características:

- Control de cruceo adaptativo
- Detección de peatones
- Detección de vehículos y ciclistas
- Frenado de emergencia automático
- Clasificación de vehículos delanteros y traseros
- Detección de señales de tráfico
- Detección de bordes de carreteras
- Advertencia de salida de carril
- Asistente de mantenimiento de carril
- Detección de semáforo
- Detección de espacio libre
- Detección de carril y límite de la carretera
- Detección de objetos

Sistema de Visión Estéreo

(Dubey, 2020) El sistema está compuesto por hardware, algoritmos y características completamente integrados y está diseñado para desafíos de conducción altamente automatizados donde no se requiere depender de la capacitación o clasificación. El sistema estéreo es una tecnología líder en la salida de información confiable y precisa de obstáculos en la carretera y detección de espacio libre para sistemas de conducción automatizada. El sistema de visión estéreo se basa en un par de cámaras altamente sincronizadas que, junto con algoritmos, son capaces de reconocer con precisión a los peatones y otros objetos a la vista del conductor. Los sistemas de visión estéreo se utilizan como un sistema redundante para radares y LiDAR con visión de futuro en sistemas de conducción automatizada. Los sistemas de visión estéreo habilitan las siguientes características:

- Control de crucero adaptativo
- Detección de vehículos, peatones y ciclistas
- Frenado de emergencia automático
- Clasificación de vehículos delanteros y traseros
- Detección de señales de tráfico
- Detección de bordes de carreteras
- Advertencia de salida de carril
- Asistente de mantenimiento de carril
- Detección general de objetos
- Vista previa de la superficie de la carretera
- Detección de espacio libre
- Asistente de estacionamiento
- Detección de objetos pequeños
- Detección de semáforo
- Detección de vehículos en cualquier ángulo
- Sistema de detección térmica

(Brooke, 2020) El sistema de detección térmica utiliza una cámara de infrarrojos montada en la rejilla delantera del vehículo que detecta diferencias de calor tan sensibles como una décima de grado para crear una imagen térmica muy detallada del mundo frente al vehículo. Una computadora a bordo (ECU) ejecuta algoritmos personalizados para detectar animales, peatones y ciclistas hasta 100 metros por delante del vehículo, el sistema reacciona y resalta si detecta animales o peatones en la pantalla del automóvil.

Los sistemas de detección térmica ayudan a los conductores a ver objetos de 3 a 4 veces más lejos que el alcance de los faros del vehículo y mejoran la visibilidad en situaciones de niebla, humo y faros delanteros.

La detección térmica habilita las siguientes características:

- Detección de peatones y ciclistas
- Detección de animales
- Frenado de emergencia automático
- Función de foco

5.3.3 LIDAR

5.3.3.1 Funcionalidad

(Warren, 2019) LIDAR significa imágenes de luz, detección y alcance. Los sensores LIDAR emiten luces láser invisible para escanear y detectar objetos en la vecindad cercana o lejana de los sensores y crear un mapa 3D de los objetos y alrededores en la pantalla de visualización. Los sensores LIDAR giran continuamente y generan miles de pulsos láser por segundo.

5.3.3.2 Funcionamiento de Características

Estos rayos láser de alta velocidad de LIDAR se emiten continuamente en los alrededores de 360 grados del vehículo y son reflejados por los objetos en el camino. Con el uso de complejos algoritmos de aprendizaje automático, los datos recibidos a través de esta actividad se convierten en gráficos 3D en tiempo real, que a menudo se muestran como imágenes 3D o mapas 3D de los objetos circundantes.

Los sensores LIDAR de automoción se pueden clasificar en dos categorías en función de la tecnología utilizada:

1. LIDAR electromecánico
2. LIDAR de estado sólido

LIDAR habilita las siguientes características:

- Control de crucero adaptativo
- Advertencia de colisión
- Sistema de prevención de colisiones
- Monitoreo de punto ciego
- Asistencia de mantenimiento de carril
- Advertencia de salida de carril
- Detección de vehículos, peatones y ciclistas
- Frenado de emergencia automático
- Clasificación de vehículos



Figura 28 Fusión del sistema LIDAR en ADAS, Texas Instruments (2018)

5.3.4 SENSORES ULTRASÓNICOS

(Stiawan et al., 2019) Un sistema de detección ultrasónica funciona transmitiendo ráfagas cortas de ondas sonoras y midiendo el tiempo que tarda el sonido en viajar a un objeto objetivo, reflejarse y regresar al receptor (Figura 2.15). La distancia al objeto es función del tiempo de viaje y la velocidad del sonido en el aire, aproximadamente 346 m / s.

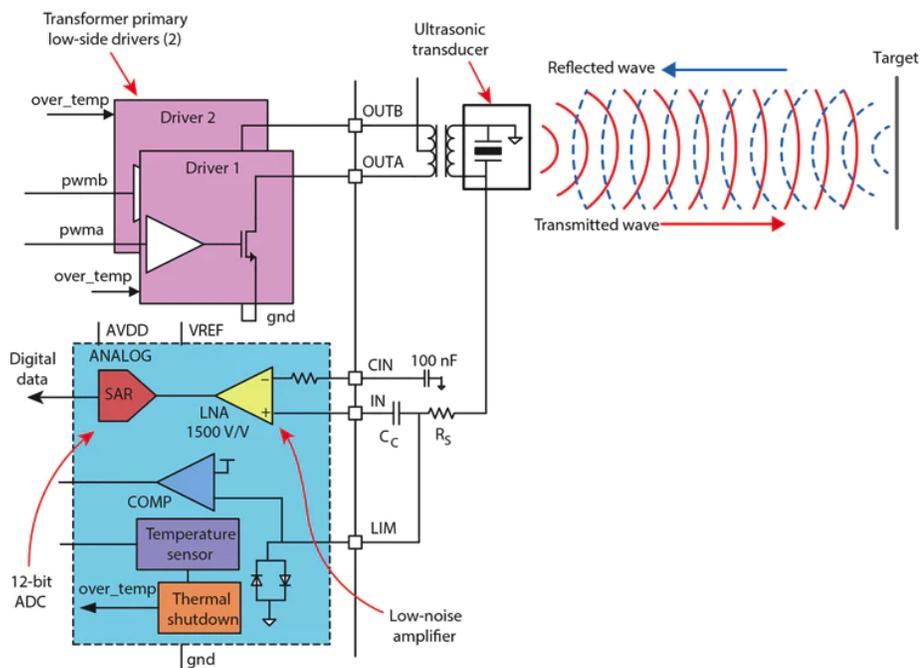


Figura 29 Fundamentos de la detección Ultrasónica, Stiawan (2019)

La detección ultrasónica se usa generalmente para aplicaciones de corta distancia a baja velocidad. Para una cobertura máxima, un sistema ultrasónico automotriz generalmente usa múltiples sensores ubicados en el espejo retrovisor y los parachoques delantero y trasero.

Su respuesta es repetible y lineal, lo que se traduce bien en representaciones visuales de la distancia del objetivo. Además, la respuesta no depende del color de la superficie.

La detección ultrasónica es un enfoque más rentable que las cámaras, que tienen una detección deficiente a corta distancia.

Aunque la detección infrarroja es más barata que la ultrasónica, es menos precisa y no puede funcionar correctamente con la luz solar directa.

ULTRASONIC habilita las siguientes características:

- Asistencia de Estacionamiento
- Parqueo Automático
- Detección de puntos ciegos
- Abridor de maletero inteligente

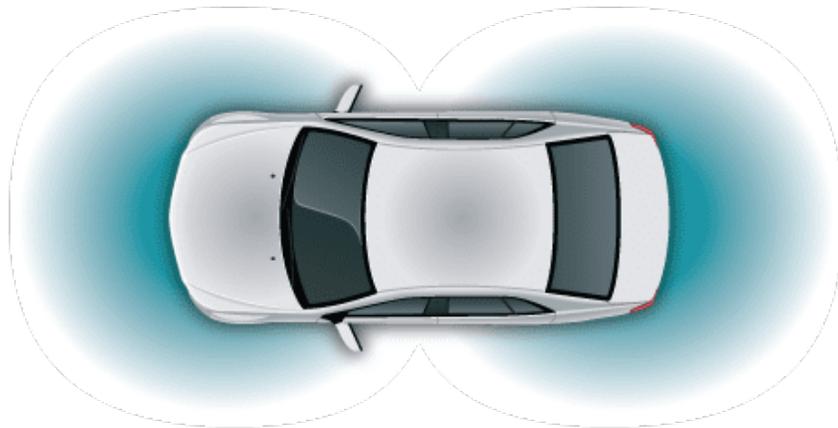


Figura 30 Fusión del sistema ultrasónico en ADAS, Texas Instruments (2018)

5.3.5 COMUNICACIÓN INALÁMBRICOS

(Smith, 2017) El estándar inalámbrico se utiliza para lograr una comunicación bidireccional en tiempo real entre vehículos (V2V) y entre vehículos e infraestructura (V2I). V2V y V2I añaden contexto al comportamiento del tráfico por carretera, como la desaceleración del objeto objetivo en una autopista. Estos sensores tienen un rango más alto que los sensores tradicionales como RADAR y sensores de video y ultrasónicos. Por lo tanto, al hacer del vehículo un nodo de comunicación, V2V y V2I amplían el alcance de los sensores ADAS tradicionales (Winner, et al. 2015). GPS o Sat-Nav son sistemas de sensores que se pueden utilizar para ADAS. Proporciona terreno, límite de velocidad y localización para asistencia en el carril.

5.3.6 FUSIÓN DEL SENSOR

(John & Mita, 2017) Permite la fusión de datos de varios sensores ambientales como radar, cámara, ultrasónico y LiDAR. Las funciones ADAS mejoradas, como la asistencia de tráfico cruzado y la evasión autónoma de obstáculos, requieren los datos de más de un sensor y la fusión de sensores correspondiente. Dado que el sistema puede tomar decisiones críticas y autónomas, la implementación de seguridad y protección es imprescindible y está respaldada por el micro controlador AURIX™ de alto rendimiento de Infineon.

Sensor Fusion permite lo siguiente:

- Crea un modelo ambiental integral al fusionar varios sensores dentro y alrededor del automóvil.
- Calcula la mejor estrategia de conducción para la máxima seguridad y comodidad del conductor.
- Toma decisiones y activa los actuadores en el automóvil.
- Permite la fusión de datos de sensores como radar, cámara, ultrasónico y LiDAR.
- Las funciones ADAS mejoradas, como la asistencia de tráfico cruzado y la evitación autónoma de obstáculos, requieren los datos de más de un sensor y la fusión de sensor correspondiente.



Figura 31 Sistema de fusión de sensores en ADAS, Texas Instruments (2018)

5.4 NIVELES DE AUTOMATIZACIÓN

(Walker, 2013) Es necesario comprender los diferentes niveles de automatización que se estandarizan en la industria automotriz. La Tabla 2 compara los niveles de SAE correspondientes a los desarrollados por el Instituto Federal de Investigación de Carreteras de Alemania (BAST) y por la Administración Nacional de Seguridad del Tráfico en las Carreteras de EE. UU. (NHTSA)

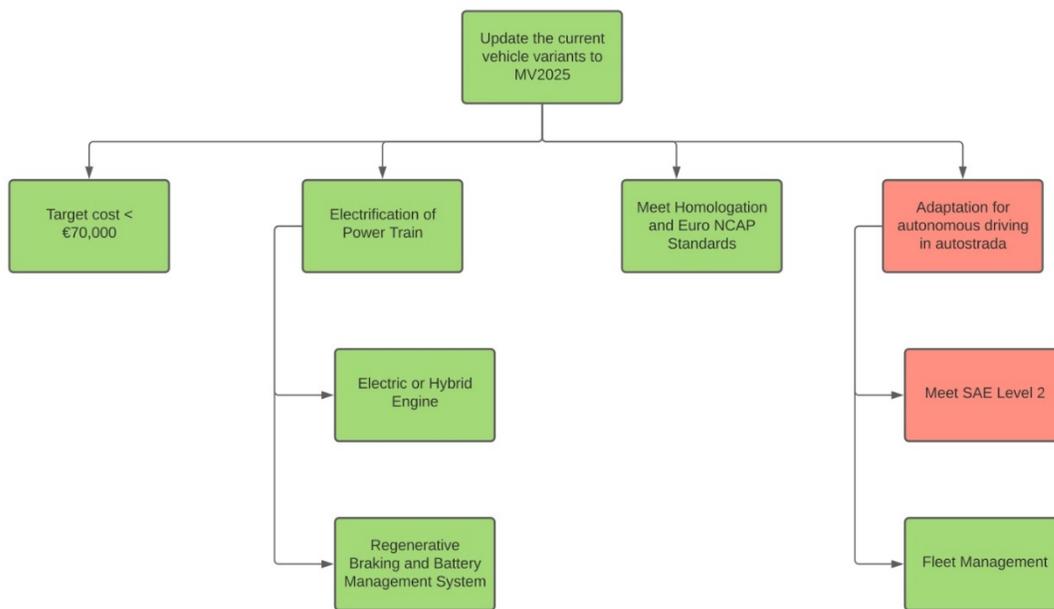


Figura 32 Árbol de objetivos para el sistema ADAS, Alexander J. (2011)

(SAE, 2018) Las tablas 2 y 3 muestran los niveles diferentes de automatización. La descripción de cada nivel se traduce en términos de funciones del vehículo ADAS para tener una mejor oportunidad de cumplir con los objetivos operativos.

5.4.1 NIVEL 0

El conductor tiene la responsabilidad total del control lateral y longitudinal del vehículo. La asistencia se presenta en forma de advertencias y alertas. Incluye advertencia de punto ciego y advertencia de colisión. Los avisos son solo una ayuda y el conductor debe estar atento en las tareas de conducción.

5.4.2 NIVEL 1

El sistema y el conductor comparten la responsabilidad del control del vehículo. El conductor es responsable del control del vehículo en todo momento, con las manos en el volante y los ojos en la carretera. El sistema realiza algunas maniobras de asistencia al control longitudinal o lateral en situaciones específicas.

Ejemplo: advertencias de colisión y sistema de mitigación de salida de carril.

5.4.3 NIVEL 2

El sistema se encarga del control del vehículo, mientras que el conductor no necesita proporcionar dirección ni accionar el pedal del acelerador. Sin embargo, la expectativa es que el conductor esté disponible para tomar el control del vehículo cuando lo requiera el sistema. También se espera que el conductor permanezca sentado en su asiento y vigile el medio ambiente. El presente nivel es la combinación de dos o más funciones del vehículo ADAS.

Ejemplo: control longitudinal y lateral en ciudad / urbano.

5.4.4 NIVEL 3

El sistema se encarga de todo el control del vehículo, el conductor esencialmente puede realizar otras tareas y mantener la vista fuera del entorno. Cuando el sistema llama debido a un evento / falla en el sistema, se espera que el conductor tome el control del vehículo. Ejemplo: control longitudinal y lateral en ciudad / entorno urbano y cambio de carril automático.

5.4.5 NIVEL 4

La diferencia clave entre la automatización de Nivel 3 y Nivel 4 es que los vehículos de Nivel 4 pueden intervenir si las cosas van mal o hay una falla del sistema. En este sentido, estos coches no requieren interacción humana en la mayoría de circunstancias. Sin embargo, un humano todavía tiene la opción de anular manualmente. Los vehículos de nivel 4 pueden operar en modo de conducción autónoma. Pero hasta que la legislación y la infraestructura evolucionen, solo pueden hacerlo dentro de un área limitada (generalmente un entorno urbano donde las velocidades máximas alcanzan un promedio de 50 km/h).

5.4.6 NIVEL 5

Los vehículos de nivel 5 no requieren atención humana: se elimina la “tarea de conducción dinámica”. Los autos de nivel 5 ni siquiera tendrán volantes o pedales de aceleración / frenado. Estarán libres de geo vallas, podrán ir a cualquier lugar y hacer cualquier cosa que pueda hacer un conductor humano experimentado. Los coches totalmente autónomos se están sometiendo a pruebas en varios rincones del mundo, pero aún no hay ninguno disponible para el público en general.

SAE level	SAE name	SAE narrative definition	Execution of steering and acceleration/ deceleration	Monitoring of driving environment	Fallback performance of <i>dynamic driving task</i>	System capability (<i>driving modes</i>)	BAST level	NHTSA level
Human driver monitors the driving environment								
0	No Automation	the full-time performance by the <i>human driver</i> of all aspects of the <i>dynamic driving task</i> , even when enhanced by warning or intervention systems	Human driver	Human driver	Human driver	n/a	Driver only	0
1	Driver Assistance	the <i>driving mode</i> -specific execution by a driver assistance system of either steering or acceleration/deceleration using information about the driving environment and with the expectation that the <i>human driver</i> perform all remaining aspects of the <i>dynamic driving task</i>	Human driver and system	Human driver	Human driver	Some driving modes	Assisted	1
2	Partial Automation	the <i>driving mode</i> -specific execution by one or more driver assistance systems of both steering and acceleration/deceleration using information about the driving environment and with the expectation that the <i>human driver</i> perform all remaining aspects of the <i>dynamic driving task</i>	System	Human driver	Human driver	Some driving modes	Partially automated	2
Automated driving system ("system") monitors the driving environment								
3	Conditional Automation	the <i>driving mode</i> -specific performance by an <i>automated driving system</i> of all aspects of the <i>dynamic driving task</i> with the expectation that the <i>human driver</i> will respond appropriately to a <i>request to intervene</i>	System	System	Human driver	Some driving modes	Highly automated	3
4	High Automation	the <i>driving mode</i> -specific performance by an <i>automated driving system</i> of all aspects of the <i>dynamic driving task</i> , even if a <i>human driver</i> does not respond appropriately to a <i>request to intervene</i>	System	System	System	Some driving modes	Fully automated	3/4
5	Full Automation	the full-time performance by an <i>automated driving system</i> of all aspects of the <i>dynamic driving task</i> under all roadway and environmental conditions that can be managed by a <i>human driver</i>	System	System	System	All driving modes		

Tabla 2 Niveles de automatización según SAE. Smith Bryant Walker, Stanford (2013)



SAE J3016™ LEVELS OF DRIVING AUTOMATION

	SAE LEVEL 0	SAE LEVEL 1	SAE LEVEL 2	SAE LEVEL 3	SAE LEVEL 4	SAE LEVEL 5
What does the human in the driver's seat have to do?	You <u>are</u> driving whenever these driver support features are engaged – even if your feet are off the pedals and you are not steering			You <u>are not</u> driving when these automated driving features are engaged – even if you are seated in “the driver's seat”		
	You must constantly supervise these support features; you must steer, brake or accelerate as needed to maintain safety			When the feature requests, you must drive	These automated driving features will not require you to take over driving	
What do these features do?	These are driver support features			These are automated driving features		
	These features are limited to providing warnings and momentary assistance	These features provide steering OR brake/ acceleration support to the driver	These features provide steering AND brake/ acceleration support to the driver	These features can drive the vehicle under limited conditions and will not operate unless all required conditions are met	This feature can drive the vehicle under all conditions	
	<ul style="list-style-type: none"> • automatic emergency braking • blind spot warning • lane departure warning 	<ul style="list-style-type: none"> • lane centering OR • adaptive cruise control 	<ul style="list-style-type: none"> • lane centering AND • adaptive cruise control at the same time 	<ul style="list-style-type: none"> • traffic jam chauffeur 	<ul style="list-style-type: none"> • local driverless taxi • pedals/ steering wheel may or may not be installed 	<ul style="list-style-type: none"> • same as level 4, but feature can drive everywhere in all conditions
Example Features						

For a more complete description, please download a free copy of SAE J3016: https://www.sae.org/standards/content/J3016_201806/

Tabla 3 SAE Levels of Driving Automation, SAE J3016 (2018)

El objetivo operativo en la **Figura 32** es cumplir con el nivel 2 de SAE y debe tener adaptación para más niveles de automatización, por lo tanto una combinación de funciones es adecuada para alcanzar los objetivos que se estudian en la sección.

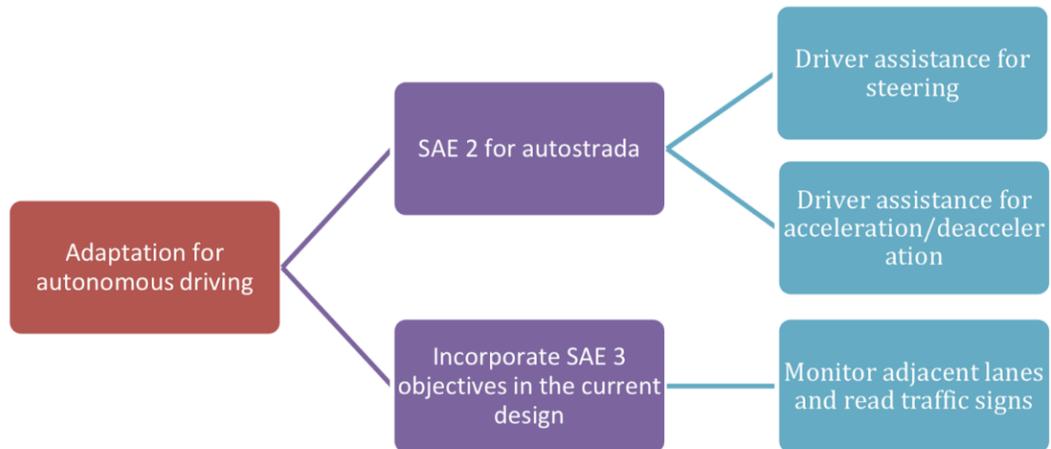


Figura 33 Objetivos operativos y sus funciones preliminares con base en la Tabla 3

Los objetivos operativos se traducen en funciones primarias del vehículo basadas en la Tabla 3. Las funciones son asistencia al conductor para la dirección, aceleración, desaceleración, monitoreo de carriles adyacentes y lectura de señales de tránsito. Las funciones adicionales de monitoreo de ángulos adyacentes y lectura de señales de tránsito facilitarán la migración de la automatización de Nivel 2 a niveles más altos de automatización (Nivel 3, Nivel 4 y Nivel 5) cuando surja la necesidad.

La necesidad del sistema se define en términos de situación operativa. Esto se hace para derivar los requisitos de los objetivos operativos y ayudar al diseño del sistema; las necesidades del sistema en la situación operativa se definen a través de la plantilla “caso de uso”. El objetivo operativo en la **Figura 33** se traduce en requisitos, que se utiliza para monitorear carriles adyacentes. El caso de uso producido en la etapa de análisis de necesidades se aplica en el diseño del sistema, la validación y durante HARA. Se debe tener cuidado de no proporcionar soluciones de diseño durante la definición del caso de uso y objetivos operativos.

5.5 CICLO DE VIDA Y SEGURIDAD AUTOMOTRIZ

La industria automotriz sigue el modelo V-Cycle **Figura 34** como ciclo de vida del sistema. El lado izquierdo de la V presenta el desarrollo del producto, mientras que el lado derecho es responsable de la integración y validación. El ciclo de vida de seguridad es un mandato de ISO26262 en la industria automotriz.

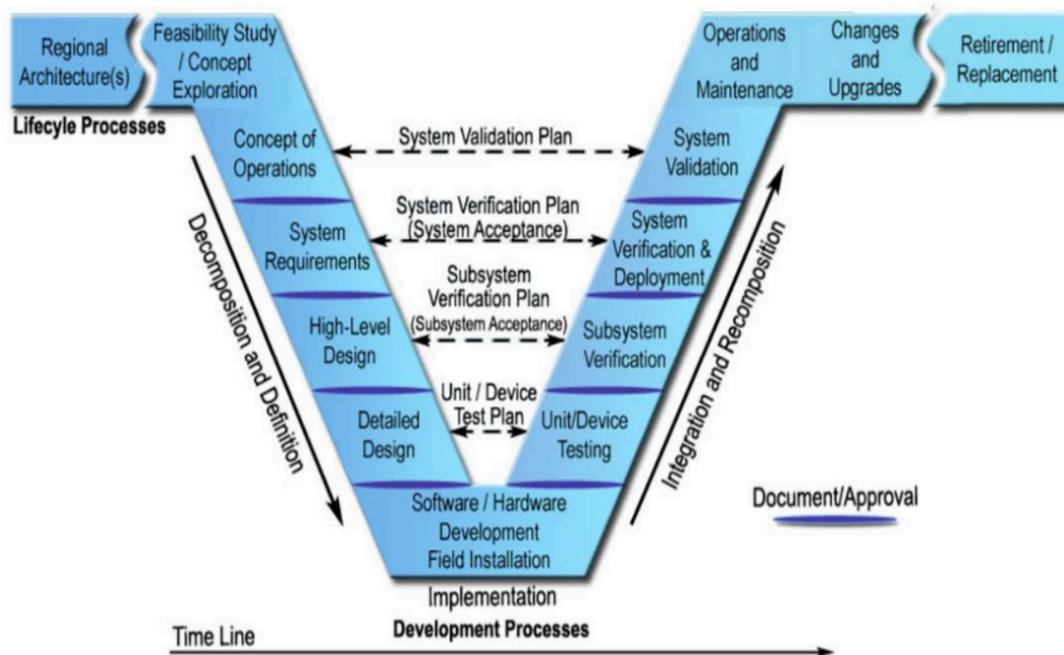


Figura 34 Modelo V para el proceso del ciclo de vida del sistema, Administración Federal de

7y

ISO26262

(ISO 26262, 2011) "LA SEGURIDAD FUNCIONAL ES LA AUSENCIA DE RIESGOS IRRAZONABLES DEBIDO A LOS PELIGROS CAUSADOS POR EL MAL FUNCIONAMIENTO DE LOS SISTEMAS E / E ".

ISO 26262 es la guía de desarrollo automotriz basada en IEC 61508, específicamente adaptada para la arquitectura E / E en vehículos de carretera. ISO 26262 se divide en 10 partes como se describe en la **tabla 4**. Se ocupa únicamente de vehículos de pasajeros.

Parte	Representación
1	Vocabulario y definición de términos utilizados en ISO 26262
2	Actividades de gestión de la seguridad
3	Actividades de la fase conceptual para derivar requisitos de seguridad
4	Diseño de producto: nivel de sistema, actividades de diseño, integración y validación
5	Desarrollo de producto - nivel de hardware: diseño, integración, validación y métricas para evaluación de fallas
6	Desarrollo de producto - nivel de software: diseño, integración, validación
7	Producción, operación, desmantelamiento, manuales de usuario, monitoreo y servicio de campo
8	Proceso de apoyo: configuración, gestión de cambios y gestión de requisitos de seguridad
9	ASH, descomposición, métodos de análisis de seguridad
10	Lineamientos: sección informativa

Tabla 4 Resumen del capítulo basado en ISO 26262 (2018)

5.5.1 PARTE 1

Esta parte está dedicada a la definición de términos que se usan comúnmente en otras partes de ISO 26262. **La Tabla 5** contiene sólo términos relevantes para esta tesis.

Glossary for ISO26262	
Item	El artículo es un sistema o combinación de sistemas, que representa funciones a nivel de vehículo.
Arquitectura	Descripción estructurada de elementos, funciones, elementos y sistemas junto con sus interfaces y límites.
Evaluación	Inspección de un artículo y representación de su nivel de confianza en el cumplimiento de la seguridad funcional.
ASIL	Nivel de integridad de la seguridad automotriz (ISO 26262, 2018); son QM, A, B, C y D se utilizan para representar la evaluación de riesgo de un artículo.
Descomposición ASIL	Realizado para reducir la ASIL de un elemento, descomponiendo las medidas de seguridad en otro elemento. Se debe tener cuidado de que haya independencia en el elemento particionado.
Controlabilidad	Medida de control sobre el artículo durante una situación crítica para evitar daños, a través de una acción oportuna en el sistema por parte del conductor o por medidas externas.
Degradación	En presencia de fallas activas, la funcionalidad del sistema se reduce de modo que se garantiza la seguridad. La degradación se logra mediante el diseño del sistema o el hardware, el software o la combinación de ambos.
Fallo Detectado	El mal comportamiento del sistema se detecta mediante la monitorización en software, hardware o la combinación de ambos.
E/E	Combinación de sistemas eléctricos y electrónicos.

Elementos	Componentes de un sistema.
Exposición	Elemento con fallas activas, operando en una situación que podría ser peligrosa.
Medida Externa	Diseño de seguridad en un artículo que mitiga algunos de los riesgos del artículo en consideración. La medida está presente fuera del límite del artículo considerado.
Fracaso	La incapacidad del artículo para realizar su tarea prevista.
Modo de Falla	Las formas en que el artículo puede fallar.
Culpa	La condición que hace que el artículo falle
Tiempo de Reacción ante Fallas	El tiempo entre la detección y para llevar el sistema a un estado seguro.
Tiempo de Tolerancia a Fallas	El tiempo máximo que el sistema puede ser confiable desde que ocurre una falla.
Seguridad Funcional	Requisitos relacionados con la seguridad, que deben implementarse además de los requisitos nominales del sistema.
Concepto Funcional	Especificación de las funciones del elemento a implementar junto con sus interacciones, límites y entorno involucrado para respetar el objetivo de seguridad.
Daño	Lesión o daño a un artículo, humano o propiedad.
Peligro	Fuente de daño
HARA	Evaluación de riesgos de análisis de peligros, una metodología a través de la cual se estudia el riesgo de un artículo a través de un evento peligroso y se clasifica con ASIL.
Evento Peligroso	Combinación de peligro y situación operativa.
Modo Operativo	Posible estado funcional del artículo durante su tiempo de funcionamiento.
Riesgo	Combinación de gravedad y ocurrencia del daño

Estado Seguro	Uno de los estados operativos del artículo, en el que el comportamiento del artículo es sin ningún riesgo no intencionado. La funcionalidad del artículo podría estar en un estado degradado.
Seguridad	La capacidad del artículo para operar de manera confiable, sin ningún riesgo en todas las situaciones.
Gravedad	Cantidad de daño a una persona o propiedad

Tabla 5 Glosario basado en ISO 26262 (2018)

5.5.2 PARTE 3

(ISO 26262, 2011) Esta parte trata del análisis del sistema en su concepción. El objetivo de esta etapa es introducir medidas de seguridad del sistema en el diseño del sistema. Los requisitos de diseño del sistema son responsables del rendimiento nominal del sistema. ISO 26262 proporciona varias cláusulas, la mayoría de las cuales son requisitos vinculantes para la definición del concepto del sistema.

5.5.2.1 CLÁUSULA 5.4.1 Propósito del Ítem

En esta etapa se definirá el propósito del ítem, especificando:

- Finalidad, funcionalidad, modos de funcionamiento y estados del artículo.
- Estándares relevantes para las funciones del artículo y limitaciones de trabajo como el todoterreno.
- Conocimientos preexistentes relacionados con los elementos que se están diseñando para lograr la funcionalidad.
- Supuestos sobre el ítem o elementos bajo consideración.
- Modos de falla conocidos y fallas.

5.5.2.2 Limitaciones de ítem

El límite del ítem se definirá en esta etapa (ISO 26262, 2011), especificando:

- Elementos del ítem, que se identifican mediante la descomposición funcional y la asignación funcional a los bloques individuales.
- Tipo de información intercambiada a través de las interfaces.
- Tipo de interfaces.
- Funcionalidad que las interfaces logran fuera de los límites del elemento y sus consecuencias.
- Funcionalidad que necesita el artículo fuera del límite para lograr las especificaciones previstas.
- Asignación de funciones que se logra mediante diferentes elementos del artículo.
- Escenarios operativos comunes en los que el artículo se utiliza durante su vida útil.

5.5.2.3 CLÁUSULA 6 Ciclo de Seguridad

(ISO 26262, 2011) Una vez que se establecen la definición del ítem y sus límites, comienza el ciclo de seguridad. En esta etapa, se comprueba el ítem para establecer si es un nuevo desarrollo o una modificación de un ítem existente.

Si se trata de una modificación de un ítem existente, se realiza un análisis de impacto, y se realiza HARA en base al análisis de impacto.

Si es un ítem nuevo, se consideran todas las especificaciones del artículo para HARA.

5.5.2.4 CLÁUSULA 7: HARA

(ISO 26262, 2011) HARA se utiliza para la determinación de los objetivos de seguridad del artículo, con el objetivo de evitar un riesgo irrazonable. Esto se hace asignando ASIL a eventos peligrosos. El ASIL es la combinación de gravedad, probabilidad de exposición y controlabilidad.

Los pasos en HARA son:

1. Análisis de la situación
2. Identificación de peligros
3. Clasificación de eventos peligrosos

5.5.2.4.1 Cláusula 7.4.2.1: Análisis de la Situación

(ISO 26262, 2011) Es la definición de las situaciones operativas del artículo; será lo más genérico posible y dentro de los límites del artículo. Sin embargo, se considerará el mal uso razonablemente previsto por parte del conductor.

5.5.2.4.2 Cláusula 7.4.2.2 Identificación de Peligros

La identificación del peligro se expresa en función del comportamiento observable a nivel del vehículo. ISO 26262 no da ninguna recomendación sobre la técnica de análisis en la identificación de los peligros.

(ISO 26262, 2011) HAZOP, análisis de fallas funcionales son las opciones tradicionales para la identificación de peligros.

5.5.2.4.3 Cláusula 7.4.2.3 Eventos Peligrosos

(ISO 26262, 2018) Los eventos peligrosos son la consecuencia de los peligros que ocurren en la peor situación posible durante la situación operativa del ítem. Se definirá la consecuencia de cada evento peligroso individual y el posible mecanismo de control disponible para el conductor para evitar eventos peligrosos.

5.5.2.4.4 Cláusula 7.4.3 Clasificación de Eventos Peligrosos

(ISO 26262, 2018) En función de las consecuencias de los eventos peligrosos, cada evento se clasifica en función de los parámetros S, E & C. Se debe proporcionar una suposición racional para la asignación de niveles S, E & C. Estas asignaciones racionales proporciona la justificación y el razonamiento detrás de la clasificación de eventos peligrosos.

5.5.2.4.4.1 Cláusula 7.4.3.2 Gravedad

(ISO 26262, 2011) La gravedad se clasifica en niveles S0, S1, S2 y S3 donde S0 corresponde a ninguna lesión y S3 corresponde a lesiones potencialmente mortales.

Rangos de Gravedad	S0	S1	S2	S3
Rango de Lesiones	Sin Lesiones	Lesión leve	Herida severa	Grave, supervivencia incierta

Tabla 6 Tabla de gravedad basada en ISO 26262 (2011)

5.5.2.4.4.2 Cláusula 7.4.3.3: Exposición

(ISO 26262, 2018) La exposición del ítem en la situación elegida se clasifica en E0, E1, E3 y E4, según su semejanza.

Rango de Exposición	E0	E1	E2	E3	E4
Rangos de Prospectos	No es probable	Muy menos probable	Menos probable	Probable	Muy Probable

Tabla 7 Tabla de exposición basada en ISO 26262 (2018)

5.5.2.4.4.3 Cláusula 7.4.3.7: Controlabilidad

Rangos de Controlabilidad	C0	C1	C2	C3
Clasificación de Rangos	En general controlable	Normalmente controlable	Generalmente controlable	Incontrolable

Tabla 8 Tabla de controlabilidad basada en ISO 26262 (2018)

5.5.2.4.4.4 Parametrización de S, E & C

S, E y C se parametrizan en base a la *Tabla 6*, *Tabla 7*, *Tabla 8*. La parametrización hace que el proceso HARA para determinar ASIL sea científico y confiable. El argumento de la parametrización utilizando un conjunto de reglas y sus prácticas se explica en detalle por (S. Khastgir et al., 2018) El argumento proporcionado, es que la interpretación subjetiva de la asignación de S, E y C a eventos peligrosos individuales se basa en el conocimiento del sistema.

Si hay una falta de comprensión del elemento bajo análisis, podría conducir a una exageración del riesgo que a su vez resultaría en un aumento de ASIL, o en el peor de los casos, socavar el riesgo de un evento peligroso, lo que frustra el propósito de HARA.

5.5.2.4.4.5 Cláusula 7.4.4.1: Determinación de ASIL

La ASIL para cada evento peligroso se determinará con base en la **tabla 9**.

Gravedad	Exposición	Controlabilidad		
		C1	C2	C3
S	E	C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S1	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S1	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Tabla 9 Guía de determinación de ASIL basada en ISO 26262 (2018)

ASIL es una combinación de la *Figura 35* de la probabilidad de exposición del vehículo a una situación operativa, el grado de capacidad de control disponible para el conductor para evitar el evento peligroso y la gravedad es el grado de lesión debido a un evento peligroso.

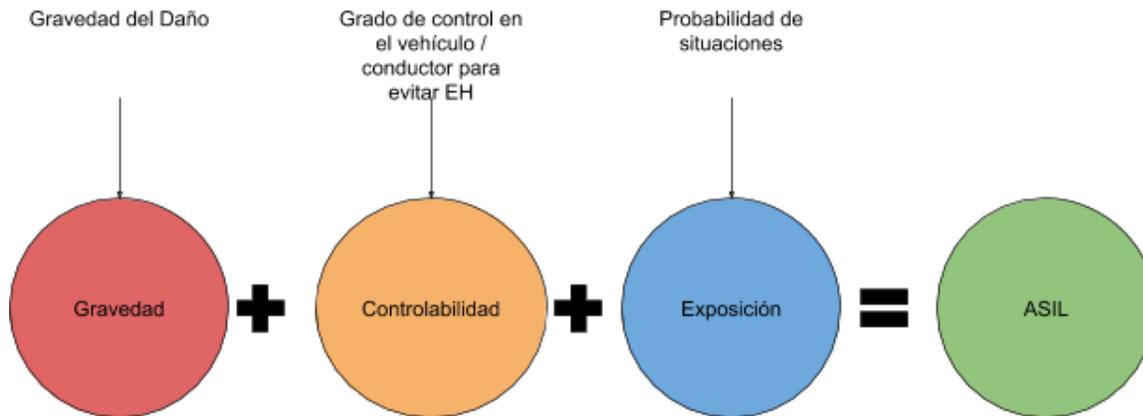


Figura 35 S, C y E según ISO 26262 (2011)

5.5.2.5 CLÁUSULA 7.4.4.3: Determinación de los objetivos de seguridad

(ISO 26262, 2018) A cada evento peligroso con ASIL se le asignará metas de seguridad. Si se determinan objetivos de seguridad similares, se combinan en un solo objetivo de seguridad. Los eventos peligrosos con el ASIL más alto tendrán prioridad sobre otros si los objetivos de seguridad son similares.

Los objetivos de seguridad pueden tener información relacionada con la transición a un estado seguro, el tiempo de tolerancia a fallas y la especificación de las características físicas máximas / mínimas de los ítems. Las metas de seguridad son el objetivo asignado al ítem, el ítem deberá tener estrategias para que las metas de seguridad no sean violadas.

5.5.2.6 CLÁUSULA 8: Concepto de seguridad funcional

(ISO 26262, 2018) El objetivo es derivar requisitos de seguridad funcional basados en los objetivos de seguridad. Cada objetivo de seguridad deberá tener uno o más requisitos de seguridad funcional. Los conceptos de seguridad funcional se derivan de mecanismos de falla específicos. En los conceptos de seguridad funcional, el requisito de seguridad funcional se asigna a los componentes funcionales lógicos de la arquitectura preliminar.

La asignación puede estar dentro o fuera del límite del elemento. La asignación fuera del límite se define como una medida externa. La *Figura 36* muestra el proceso de los objetivos de seguridad y la derivación de la seguridad funcional.

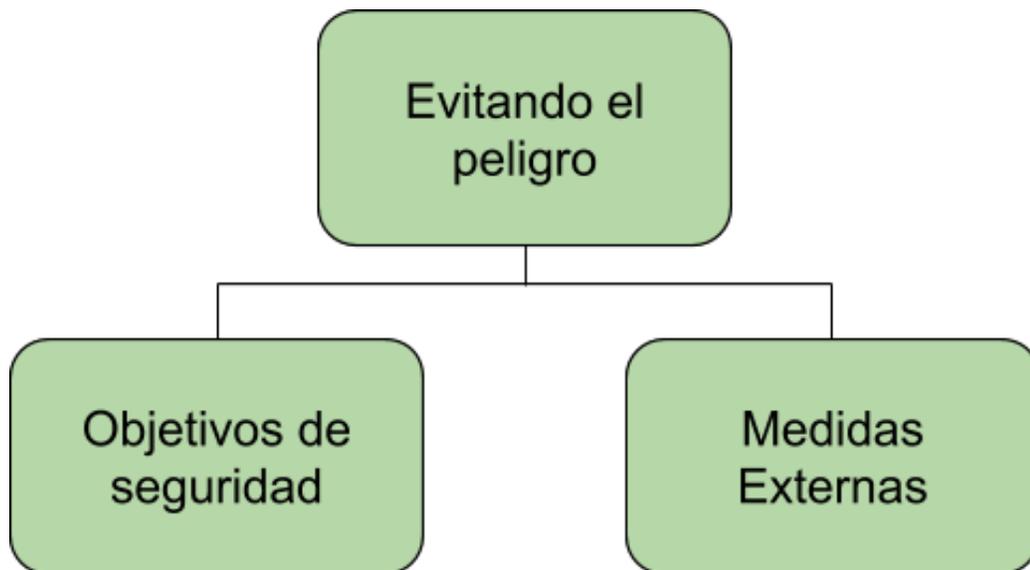


Figura 36 Seguridad a través de medidas externas basadas en ISO 26262 (2018)

(ISO 26262, 2018) El enfoque básico de la seguridad funcional es la reducción del riesgo, en base a su definición: el riesgo es la combinación de la probabilidad de que ocurra un daño y la gravedad de ese daño.

En esta tesis se estudia la reducción de la ocurrencia de daños mediante la inclusión de medidas de seguridad. ASIL es la estimación en esfuerzo / costo que se necesita en la reducción del riesgo para llevar el riesgo a un nivel aceptable, por lo tanto, si un riesgo se clasifica en una posición alta según un enfoque conservador, el ítem podría terminar teniendo más seguridad de la necesaria y un mayor costo.

5.5.3 PARTE 3 ISO 26262: “METODOLOGÍA”

Las actividades de la Parte 3 se resumen en la siguiente metodología:

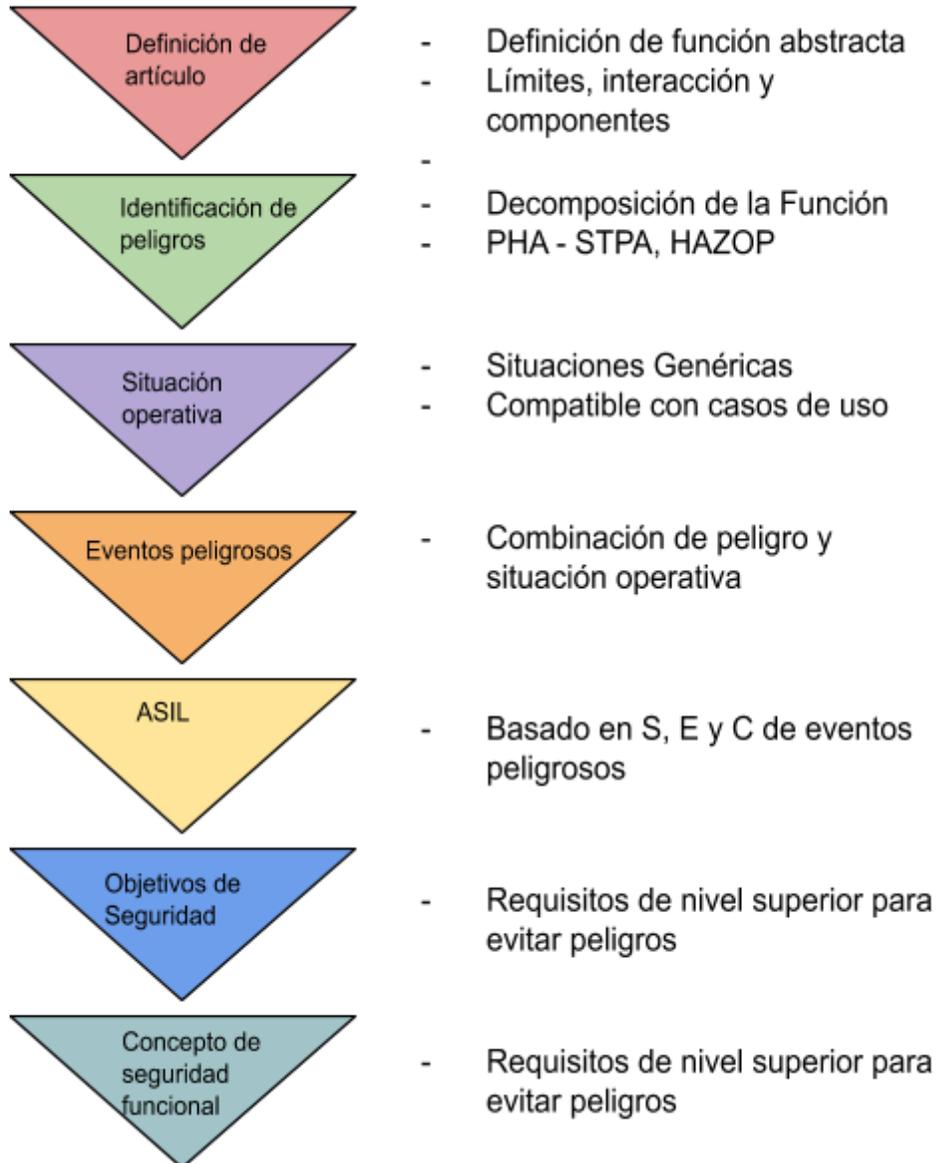


Figura 37 Metodología de la fase conceptual de ISO 26262, basada en ISO 26262 (2018)

5.5.4 SISTEMA Y SEGURIDAD PARA LA FASE DE CONCEPTO

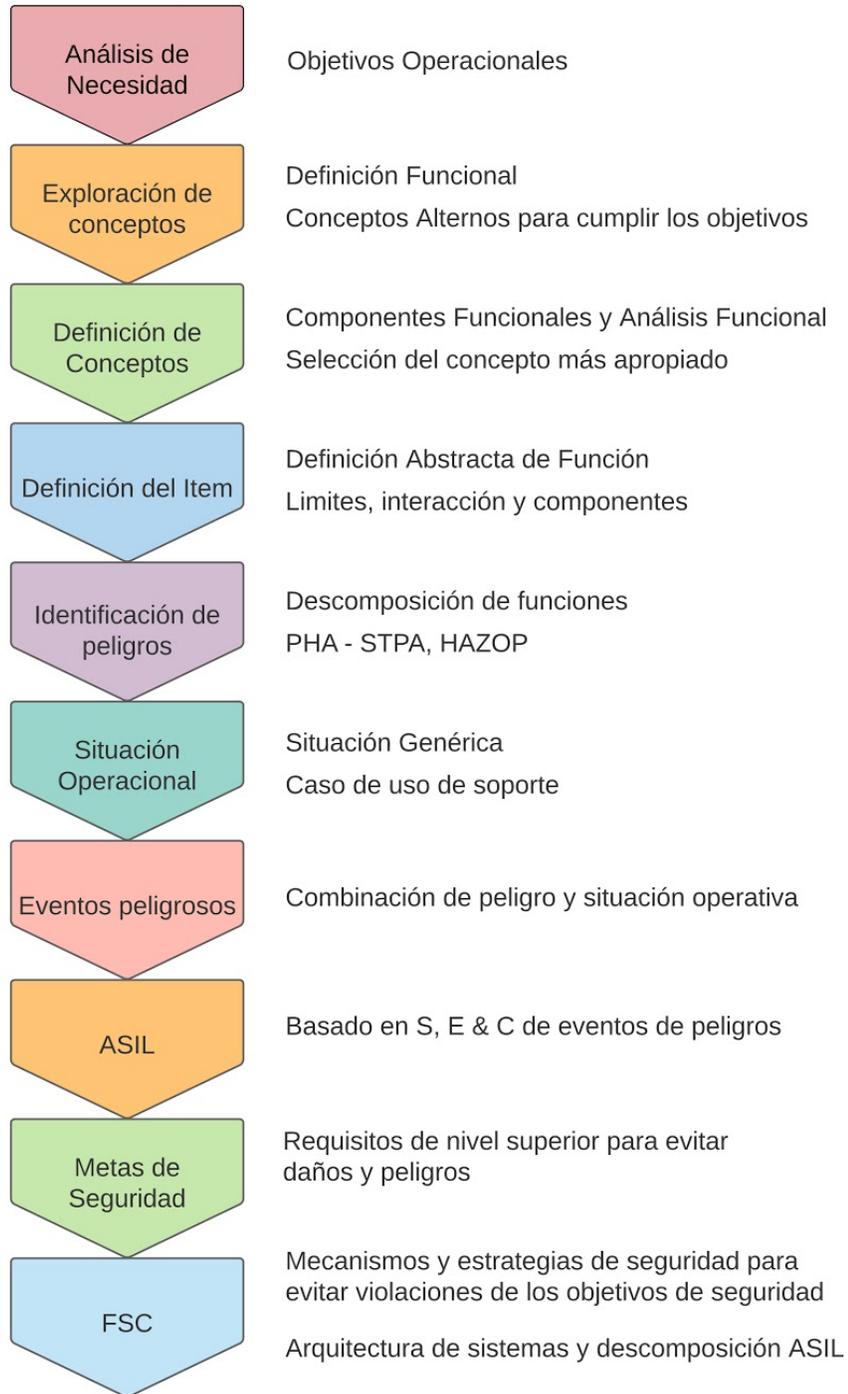


Figura 38 Metodología de ciclo de vida de seguridad e ingeniería de sistemas derivados, basada en ISO 26262 (2018)

6. METODOLOGÍA

6.1 MATERIAL Y MÉTODO

En la realización del Análisis de Seguridad y Evaluación de Riesgos para el sistema ADAS en Vehículos Volvo adecuado a la norma de seguridad proporcionada por ISO26262, la cual se utilizará como marco de referencia para esta investigación mostrado en la *Figura 37* se requiere la identificación del tipo de estudio, las variables a utilizar, la descripción de los instrumentos y obtención de información, llevando a cabo la metodología siguiente:

6.2 TIPO DE ESTUDIO

El presente informe de investigación cumple con las características de un estudio de tipo analítico ya que se desglosan las situaciones de peligro, así como los ítems a analizar lo que permite ejecutar un entendimiento superior, recolectando y comprendiendo la vinculación entre distintos actuadores, resultando en un conocimiento completo y preciso sobre lo analizado. Teniendo en cuenta la naturalidad de los métodos de análisis presentes en esta investigación, cumple también con las características de un estudio de tipo descriptivo, ya que se mide de manera independiente las variables y se muestra la información que describe las situaciones analizadas, desarrollando así el proceso de investigación.

Este estudio tienen como principal objetivo el desarrollo de un análisis completo de seguridad y detección de riesgos asociados al funcionamiento de ADAS en vehículos Volvo y su uso, basados en el marco de referencia de seguridad brindada por ISO 26262. El trabajo investigativo se cataloga dentro de la normativa para la organización, realización y evaluación de Forma de Culminación de Estudio como un trabajo de monografía, el cual está enfocado a establecer objetivos de seguridad que fomenten la extensión de las capacidades actuales del sistema ADAS.

Por tanto la profundidad de la investigación es exploratoria / descriptiva debido a que se realiza un reconocimiento de las capacidades actuales de ADAS a nivel de componentes, además de la identificación de escenarios peligrosos y el análisis de fallas para cada uno de los ítems, que puedan afectar la operatividad del sistema y conllevar a un mayor riesgo para el conductor y el vehículo.

6.3 DEFINICIÓN OPERACIONAL DE LAS VARIABLES

Matriz para la definición operacional de las variables						
Variable	Tipo de Variable	Definición de la Variable	Indicador	Reactivo/ Item	Técnica e instrumento	Fuente de Información
Falla Detectada a nivel de sistema	Nominal Categorica	Evaluar el impacto de fallas o riesgos provocados por el malfuncionamiento de componentes del sistema.	NPR: Modos de Falla Efectos Causa	Promedio del Número de Riesgo con rango tipo de formato numerico 0 – 10 de las fallas detectadas. Ver tabla 17.	FMEA	Reporte fallos ADAS - Volvo en vehiculos comerciales. Reportes de Simulaciones
Nivel de Riesgo asociado al evento peligroso analizado	Nominal Politómica / Numérica	Identificar el mal funcionamiento de componentes o mala actuación del conductor que conduce a un escenario peligroso y la evaluación del riesgo de tal.	ASIL: Severidad Exposición Controlabilidad	Nivel automotriz de seguridad integral con rango tipo de formato en escala de riesgo: QM – D. Aplicación Ver tabla 26.	HARA	Base de datos de simulaciones y reportes de usuarios. Observación de CCTV.

Tabla 35 Matriz Operacional de Variables

6.4 POBLACIÓN Y MUESTRA

En la presente investigación se aborda los vehículos Nivel 2 / 3 de automatización, por lo tanto, la población a analizar son los vehículos Volvo con dichos niveles, los cuales han sido establecidos como vehículos comerciales desde el año 2019 hasta la fecha actual, modelos 2020 – 2021. La realización de la muestra se llevará a cabo en la sede central de Volvo Cars y Zenuity en la ciudad de Gotemburgo, a partir de casos documentados de tipo sistemático en la región de Suecia. Las muestras obtenidas presentan características específicas al estudio realizado al estar directamente relacionadas con fallas en el sistema de ADAS, lo que permite analizar: registro de fallas en el sistema ADAS de vehículos en proceso de validación, reportes de fallas asociados con ADAS de vehículos en taller central y datos obtenidos de los distintos escenarios y reproducción de escenarios identificados en la investigación en las plataformas de simulación.

6.5 INSTRUMENTOS DE RECOLECCIÓN DE DATOS

Los principales instrumentos de recolección de datos que serán utilizados son las escalas de medición presentadas que han sido proporcionadas por ISO 26262 (2018) y el manual de la implementación de tales métodos de análisis que se utilizarán acorde a las sugerencias brindadas por el manual del estándar. Los registros de observación son un instrumento principal en la evaluación de riesgos y con el que se desarrollará el estudio. De igual manera, se han organizado reuniones en las cuales se ha discutido y desarrollado análisis de las muestras, en conjunto con la colaboración grupal de expertos de distintas áreas: Desarrollo de Software, Arquitectura de Interfaz, FuSa (Seguridad Funcional) y R&D. Es necesario y se sugiere contar con la participación de especialistas con experiencia en el campo de seguridad funcional, para poder realizar el análisis HARA de forma subjetiva bajo criterios consensuados. Para complementar este estudio se colaboró con Zenuity en el desarrollo de simulaciones de los eventos peligrosos más relevantes en los programas, MatLab / Simulink & CARLA.

Programas utilizados en esta investigación:

N	Nombre	Utilidad del Programa
1	C++	Lenguaje utilizado por Zenuity para programar las simulaciones en 3D
2	LucidChart	Desarrollo de Figuras y Flujogramas
3	Excel	Desarrollo de tablas calculo y base de datos de estudio
4	MatLab	Plataforma para recrear escenarios peligrosos de manera básica y consideración principal es el vehículo ego.
5	Simulink	Extensión de Matlab para recrear escenarios peligrosos y operatividad de vehículo ego.
6	CARLA	Plataforma de Fuente abierta, para recrear escenarios completos con agentes externos y analizar el vehículo ego.

6.5 ANÁLISIS Y PROCESAMIENTO DE LA INFORMACIÓN

Las técnicas a utilizar para organizar, clasificar y analizar la información son brindadas por ISO 26262 y por el manual de los dos métodos analíticos: FMEA - HARA. Se proporciona una tabla de riesgo en el que se identificará y categoriza el nivel de peligrosidades de cada falla del sistema (ASIL).

Estos riesgos se estudian a fondo mediante observación y análisis del comportamiento de conductor - interfaz y se identifican los requisitos de alto nivel para elaborar metas de seguridad funcional que el sistema tiene que cumplir. Y finalmente, se tratarán las fallas en el diseño operacional del sistema y se evaluará con un enfoque sistemático, priorizando el control dinámico de los componentes y actuadores, como el principal punto de estudio.

Consideraciones Éticas

De acuerdo con los principios establecidos en la norma ISO 26262(2011:2018) Marco de Referencia de Seguridad en componentes E/E automotriz y en el marco de referencia establecido por la Comisión de Movilidad y Transporte en Seguridad Vial Edición 2011 – 2020 y debido a que esta investigación se consideró como una auditoria de seguridad y asesoramiento de riesgos en el sistema ADAS, este estudio se desarrollará conforme a los siguientes criterios:

- Explicar brevemente los principios éticos que justifican la investigación de acuerdo a una normativa a nivel internacional (WHO, SAE) y a nivel local (EU).
- Fundamentar si la simulación se realizó en plataformas digitales o en físico (en vías públicas).
- El conocimiento producido no puede obtenerse por otro medio idóneo.
- Los riesgos de participar en esta investigación son expresados y las garantías de seguridad se brindan a todos los participantes.
- Se cuenta con el consentimiento informado y por escrito de los equipos de Zenuity / Volvo Cars que participaron en esta investigación bajo la resolución
- Contar con el Consentimiento Informado y por escrito del sujeto de investigación o su representante legal con las excepciones dispuestas en la Resolución en la Carta de los Derechos Fundamentales de la Unión Europea y en el Convenio de Oviedo.
- Se relacionó la experiencia de los investigadores y el marco de estudio de la investigación
- Se establece que la investigación se llevará a cabo cuando se obtenga la autorización: de la institución donde se realice la investigación.

Validez y Confiabilidad de los instrumentos

En el presente trabajo monográfico se ha colaborado con distintos grupos / departamentos de la empresa Zenuity para la elaboración de los análisis propuestos. Según ISO 26262 (2018), las valoraciones de seguridad funcional no pueden ser realizadas por un único equipo de seguridad funcional. Por el contrario, nos sugiere como marco de referencia realizar dichos análisis de manera grupal, con el apoyo de expertos en seguridad funcional con mundología relevante que puedan contribuir con su experiencia pasada en el desarrollo del estudio.

El propósito del consenso grupal es principalmente ampliar el enfoque del análisis, para tomar en consideración distintas variables, que se pretende discutir en sesiones de análisis grupal. Esta práctica es un aporte para validar los resultados. Al practicar el análisis con un alto nivel de redundancia, trae como resultado un alto nivel de confiabilidad, que permite verificar antes de desarrollar simulaciones o incluso proyectarlo a un nivel superior como es la etapa de desarrollo del producto.

En las tablas de *Anexo 11 – 14*, se presentan una rúbrica de validación de los instrumentos y programas utilizados en esta investigación, realizada de manera grupal y avalada por el jefe de departamento de cada uno de los equipos con los que se colaboró para la realización de esta investigación (Dpto. FuSa, Dpto. Software Development, Dpto. Diseño de Interfaz (UX & UI) & Dpto. R&D).

7. RESULTADOS Y DISCUSIÓN

ANÁLISIS DE SEGURIDAD DEL SISTEMA

En este capítulo se implementarán las herramientas de análisis propuestas a los eventos de riesgo en respecto a vehículos con funciones de Nivel 2 de automatización. En el primer método (FMEA) se identificarán fallas y posibles causas a nivel de sistema. En el segundo método (HARA) se analizarán las fallas a nivel de componentes en el sistema o en el interfaz hombre – máquina (HMI) y finalmente se identificarán las limitaciones de seguridad y los escenarios que conducen a dichas violaciones de las limitaciones resultando en propuestas y recomendaciones en la fase conceptual y de diseño. El resultado es la elaboración de objetivos de seguridad por cada uno de los eventos de riesgo, que posteriormente se traducirán en requisitos de seguridad funcional en la fase de desarrollo del vehículo.

7.1 FMEA

(ASQ, 2015) El análisis de modos y efectos de falla (FMEA) es un enfoque estructurado para descubrir fallas potenciales que pueden existir dentro del diseño de un producto o proceso. Los modos de falla son las formas en que un proceso puede fallar. Los efectos son las formas en que estas fallas pueden generar desperdicio, defectos o resultados perjudiciales para el usuario.

El análisis de modos y efectos de falla está diseñado para identificar, priorizar y limitar estos modos de falla. FMEA no sustituye a la buena ingeniería. Más bien, mejora la buena ingeniería aplicando el conocimiento y la experiencia de un Equipo Interfuncional (CFT) para revisar el progreso del diseño de un producto o proceso y evaluando su riesgo de falla.

7.1.1 CRITERIOS DE PRIORIDAD DE RIESGO

Existen tres criterios de prioridad de riesgo, que sirven para calificar el nivel de riesgo. Se basan en criterios tales como gravedad, ocurrencia y detección. El resultado de estos tres criterios es el Número de Prioridad de Riesgo (NPR).

7.1.1.1 Severidad / Gravedad

(Zigmund Bluvband & Pavel Grabov, 2009) Que califica la severidad del efecto potencial de la falla.

GRAVEDAD	CRITERIO	VALOR
Muy Baja Repercusiones imperceptibles	No es razonable esperar que este fallo de pequeña importancia origine efecto real alguno sobre el rendimiento del sistema. Probablemente, el conductor ni se daría cuenta del fallo	1
Baja Repercusiones irrelevantes apenas perceptibles	El tipo de fallo origina un ligero inconveniente al conductor. Probablemente, este observará un pequeño deterioro del rendimiento del sistema sin importancia. Es fácilmente subsanable	2-3
Moderada Defectos de relativa importancia	El fallo produce cierto disgusto e insatisfacción en el cliente. El conductor observará deterioro en el rendimiento del sistema	4-6
Alta	El fallo puede ser crítico y verse inutilizado el sistema. Produce un grado de insatisfacción elevado	7-8
Muy Alta	Modalidad de fallo potencial muy crítico que afecta el funcionamiento de seguridad del producto o proceso y/o involucra seriamente el incumplimiento de normas reglamentarias. Si tales incumplimientos son graves corresponde un 10	9-10

Tabla 10 Escala de gravedad de cinco puntos, Bluvband & Grabov (2009)

7.1.1.2 Ocurrencia

(Zigmund Bluvband & Pavel Grabov, 2009) Que califica la probabilidad de que ocurra la falla.

FRECUENCIA	CRITERIO	VALOR
Muy baja improbable	Ningún fallo se asocia a procesos casi idénticos , ni se ha dado nunca en el pasado, pero es concebible	1
Baja	Fallos aislados en procesos similares o casi idénticos. Es razonablemente esperable en la vida del sistema, aunque es poco probable que suceda.	2-3
Moderada	Defecto aparece ocasionalmente en procesos similares o previos al actual. Probablemente aparecerá algunas veces en la vida del componente/sistema.	4-6
Alta	El fallo se ha presentado con cierta frecuencia en el pasado en procesos similares o previos procesos que han fallado.	7-8
Muy Alta	Fallo casi inevitable. Es seguro que el fallo se producirá frecuentemente	9-10

Tabla 11 Escala de ocurrencia de cinco puntos, Bluvband & Grabov (2009)

7.1.1.3 Detección

(Zigmund Bluvband & Pavel Grabov, 2009) Que califica la probabilidad de que el problema se detecte antes de que llegue al usuario final.

Puntaje	Descripción	Criteria
1	Muy bajo o ninguno	Molestia menor
2	Baja o menor	Producto operable con rendimiento reducido
3	Moderado o significativo	Degradación gradual del rendimiento
4	Alto	Pérdida de función
5	Muy alto o catastrófico	Relacionado con la seguridad Fallos catastróficos

Tabla 12 Escala de detección de cinco puntos, Bluvband & Grabov (2009)

7.1.2 MATRIZ DE RIESGO

A continuación se clasificaron los eventos peligrosos de acuerdo al nivel de riesgo, este modelo está basado en las variables de probabilidad de que el evento ocurra y las consecuencias de este. El resultado es un nivel de riesgo para cada uno de los eventos. Esto permite estudiar más a fondo aquellos eventos peligrosos que han resultado con un alto nivel de riesgo y en base a este nivel, posteriormente se analizará en detalle mediante el análisis HARA. En esta tesis se estudiarán todos los eventos, pero existe un mayor enfoque a los eventos de mayor riesgo.

Desvinculación del sistema al tomar curvas o giros cerrados

- Evento 1: Desvinculación del Sistema al tomar una curva al momento de salir de una rampa.
- Evento 2: Fallo en el sistema al tomar una curva pronunciada
- Evento 3: Fallo del sistema al no poder estimar las líneas límites de carril y desvinculación durante maniobra de curva
- Evento 4: Fallo en el sistema de centrado y fijado de carril

Fallo de detección de señales horizontales y MOT

- Evento 1: Fallo en el reconocimiento de salidas (carriles)
- Evento 2: Fallo en el reconocimiento de objetos múltiples
- Evento 3: Fallo en accionar protocolo de choques

Situaciones Climáticas

- Evento 1: Límites de carretera cubierto por nieve
- Evento 2: Fallo en el reconocimiento de objetos múltiples
- Evento 3: Mal Funcionamiento producto a baja visibilidad

Ambientes Urbanos

- Evento 1: Intersecciones de 4 via
- Evento 2: Fallo en evasión de peatones y objetos parqueado
- Evento 3: Fallo en maniobras de rotonda (varias)

PROBABILIDAD

CONSECUENCIA

	Muy poco probable que suceda	Poco Probable que suceda	Posible - mente podría pasar	Probable que suceda	Muy probable que suceda
Catas - trófico (Fatal)					
Mayor (Discapa - cidad permanen - te)					
Moderado (Hospita - lización)				Evento 3	
Menor (Primeros Auxilios)				Evento 2	
Superficial (Trata - miento no requerido)		Evento 4	Evento 1		

Tabla 13 Matriz de Riesgo Desvinculación del Sistema al Tomar Curvas

BAJO MEDIO ALTO

PROBABILIDAD

	Muy poco probable que suceda	Poco Probable que suceda	Posible - mente podría pasar	Probable que suceda	Muy probable que suceda
Catas - trófico (Fatal)					
Mayor (Discapa - cidad permanen - te)			Evento 3		
Moderado (Hospita - lización)					
Menor (Primeros Auxilios)			Evento 2	Evento 1	
Superficial (Trata - miento no requerido)					

Tabla 14 Matriz de Riesgo Señales Horizontales y MOT

PROBABILIDAD

	Muy poco probable que suceda	Poco Probable que suceda	Posible - mente podría pasar	Probable que suceda	Muy probable que suceda
Catas - trófico (Fatal)					
Mayor (Discapa - cidad permanen - te)					
Moderado (Hospita - lización)				Evento 2	Evento 3
Menor (Primeros Auxilios)					
Superficial (Trata - miento no requerido)			Evento 1		

Tabla 15 Matriz de Riesgo Situaciones Climáticas

PROBABILIDAD

	Muy poco probable que suceda	Poco Probable que suceda	Posible - mente podría pasar	Probable que suceda	Muy probable que suceda
Catas - trófico (Fatal)					
Mayor (Discapa - cidad permanen - te)					
Moderado (Hospita - lización)				Evento 1	Evento 2
Menor (Primeros Auxilios)					
Superficial (Trata - miento no requerido)					Evento 3

Tabla 16 Matriz de Riesgo Ambiente Urbanos

7.1.3 PROCESO FMEA

En la siguiente tabla se desarrolla el análisis FMEA, donde se identifican los fallos potenciales, sus efectos y posibles causas del modo de fallo. El primer paso para este análisis de modo de fallo es describir la función de los ítems, así como la identificación de modos de fallo.

Se solicitó la colaboración de oficiales de seguridad del departamento de seguridad funcional de Zenuity, en donde se abordó los ítems de manera grupal mediante una sesión creativa, en la cual se han establecido los puntajes del NPR en el estado actual de los ítems. Así como propuestas para acciones correctoras para dichas fallas, para las cuales se han evaluado el puntaje con dichas acciones implementadas.

Se realizarón simulaciones de los escenarios peligrosos (ver anexos), en donde se muestra la plataforma de simulación de Simulink corriendo en una vista 3D distintos escenarios peligrosos, analizados en esta investigación. Las simulaciones en la empresa de Zenuity se desarrollan en la plataforma de fuente abierta - CARLA, para complementar cualquier escenario no definido o inusual y poner en práctica los algoritmos y los controladores del sistema.

Simulaciones de escenarios de tráfico permite que los oficiales de seguridad puedan detectar mal funcionamiento en los controladores al permitirles realizar demostraciones en circuitos cerrados y así traducir las fallas o desvinculaciones que resultan en requisitos funcionales para que los programadores de algoritmos e ingenieros en software puedan implementarlo en el sistema. La recolección de datos mediante simulaciones de prueba en escenarios reales permite recolectar datos de eventos inusuales y posteriormente analizarlos en el laboratorio.

FUNCIÓN DEL ÍTEM	FALLOS POTENCIALES				ESTADO ACTUAL				ACCIÓN CORRECTORA	RESPONSABLE	SITUACIÓN DE MEJORA					
	ÍTEM #	MODOS DE FALLO	EFECTOS	CAUSAS DEL MODO DE FALLO	MEDIDAS DE ENSAYO	G.1- 10	F.1- 10	D.1- 10			NPR	ACCIONES IMPLANTADAS	G.1- 10	F.1- 10	D.1- 10	NPR
Control Lateral / Longitudinal	1	El desvinculo del sistema en curvas con líneas horizontales poco visibles o desgastadas	Intervención humana a último momento	Sensores no pueden detectar líneas de límite desgastadas	Ensayos en escenario virtual	6	5	7	210	Implementación de proyección virtual de líneas límites	2	5	9	90		
	2	El desvinculo del sistema en carreteras con curvas tipo zigzag's	Intervención humana a último momento	Sistema no desarrollado para carreteras zigzag's	Ensayos en escenario virtual	9	8	4	288	Mejoramiento de las capacidades de control lateral para manejar distintos tipos de curvas	7	4	8	224		
	3	El desvinculo del sistema en curvas cerradas.	Intervención humana a último momento	Sistema lucha para realizar la maniobra pero falla	Ensayos en escenario virtual	9	6	7	378	Mejoramiento de las capacidades de control lateral para manejar distintos tipos de curvas	5	6	7	210		
Condiciones Climáticas	4	El sistema falla al determinar las líneas límites y ubicación de carril en condiciones de nieve	Fallo en el sistema	Nieve cubre un % de área de los límites de los carriles externos en carril vecino.	Ensayos en escenario virtual	4	8	4	128	Implementación de proyección virtual de líneas límites	2	7	8	112		
	5	El sistema falla al determinar las líneas límites y ubicación de carril en condiciones lluviosos	Intervención humana a último momento	Mantos de agua cubre un % de área de los límites de los carriles externos.	Ensayos en escenario virtual	7	9	2	126	Implementación de proyección virtual de líneas límites	4	5	7	140		
	6	El sistema falla al ajustar posicionamiento conforme al objeto	Fallo en el sistema	Nebulina principal causa de fallos en ambientes de baja visibilidad	Ensayos en escenario virtual	10	8	3	240	Implementación de proyección virtual de líneas límites	7	7	7	343		
Ambiente Urbanos	7	Detección de Objetos Múltiples e inusuales	Detecciones Imperfectas	Estado del objeto desconocido	Ensayos en escenario virtual	5	7	3	105	Implementar entrenamiento de categorización de objetos varios e inusuales	2	4	7	56		
	8	Maniobras usuales en escenarios urbanos	Detecciones Imperfectas	Sistema no apto para manejar alrededor de un objeto obstruyendo parte de las vías	Ensayos en escenario virtual	3	7	4	84	Entrenar al sistema a maniobrar en ambientes urbanos de manera segura	2	4	8	64		
	9	Maniobras en rotondas	Intervención humana a último momento	No desarrollado para rotondas	Ensayos en escenario virtual	4	10	2	80	Desarrollar algoritmos que le permitan al sistema a maniobrar en rotondas	3	8	5	120		

Tabla 17 FMEA Proceso - ADAS

7.2 HARA

7.2.1 DEFINICIÓN DE ÍTEMS

7.2.1.1 Descripción de Ítems

Los componentes del sistema a evaluar son LIDAR, sensores de video, comunicación inalámbrica, SRR - R / SRR - L y EPS. La comunicación entre los componentes dentro del ítem y los elementos externos es hecho a través del Controlador de Red de Zona (CAN).

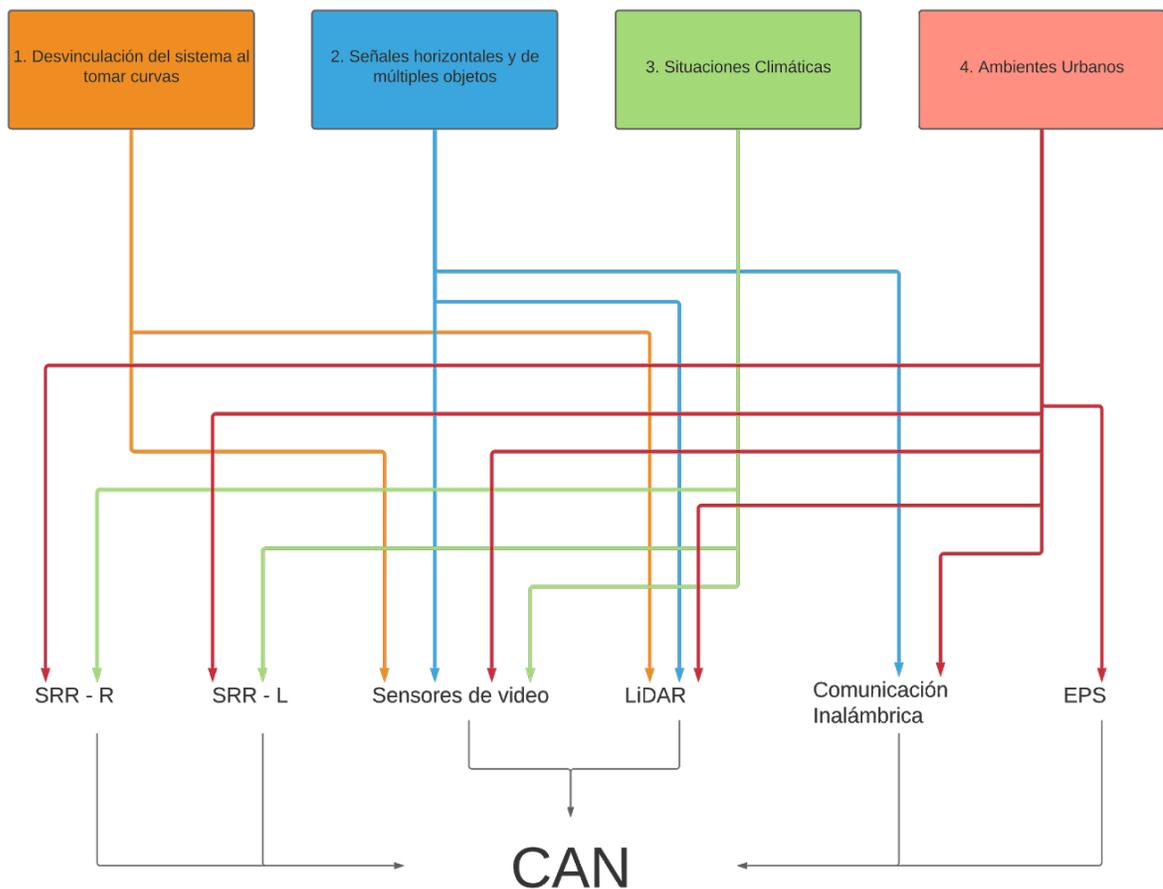


Figura 39 Relación entre ítems y elementos externos por medio de CAN

7.2.1.2 Propósito

El propósito del ítem es mantener una distancia segura del objetivo en movimiento frente al vehículo mientras se localiza en el centro del carril. El ítem también mostrará los límites de velocidad de la señal de tráfico y advertirá si los carriles adyacentes están ocupados antes de una maniobra de cambio de carril por parte del vehículo ego.

7.2.1.3 Funcionalidad de Ítems

La funcionalidad del ítem se basa en la discusión en la etapa de exploración del concepto, las funcionalidades son las siguientes:

- El ítem utilizará información de los sensores para mantener el vehículo a la velocidad y carril definido por el conductor. También permitirá al conductor reducir / aumentar la velocidad y cambio de carril.
- El ítem deberá monitorear el medio ambiente. Si hay un vehículo objetivo que se mueve más lento, entonces el ítem mantendrá el vehículo en el mismo carril y mantendrá una distancia segura del objeto objetivo después de alertar al conductor.
- El ítem permitirá al conductor tomar el control del vehículo ego, reducir / aumentar la distancia segura y cambiar de carril cuando está siguiendo un objetivo.
- El ítem debe monitorear una maniobra de cambio de carril y advertir al conductor sobre el vehículo en movimiento en sus regiones de punto ciego.
- Los ítems deberán exhibir las señales de tráfico vertical y horizontal, así como las alimentadas por la comunicación con el sistema GPS.

7.2.1.4 Modos y Estados de Funcionamiento

Modo Operativo	Estado Operativo	Funcionalidad
APAGADO	Elemento no encendido.	NA
ENCENDIDO / PASIVO	El artículo espera la velocidad y distancia establecidas válidas.	Validar los datos y monitorear si la velocidad del vehículo es superior a 30 km / h
ENCENDIDO / SEMI ACTIVO	El artículo mantiene la velocidad definida y el conductor es responsable de la dirección.	Supervisar los posibles objetos, señales de tráfico, puntos ciegos y marcas de carriles. Comprobar si la velocidad del vehículo es superior a 50 km / h
ENCENDIDO / ACTIVO	El artículo mantiene la distancia segura y es responsable de la dirección.	Siga el objetivo, controle la marca del carril, las señales de tráfico y el punto ciego. Compruebe si la velocidad del vehículo es superior a 50 km / h
ENCENDIDO / COMPLETAMENTE ACTIVO	Los elementos deben mantener una distancia segura y guiar al vehículo en el centro del carril.	Ítem mantiene la distancia segura y mantiene el vehículo en el carril, monitorea la solicitud de cambio de carril y advierte al conductor si el punto ciego está ocupado. Verifique la presencia del conductor en el asiento del

		conductor.
ENCENDIDO / PASIVO	El artículo entrega el control del vehículo al usuario	Supervisa el punto ciego, la señal de tráfico y la velocidad del vehículo y espera la entrega del control.
ENCENDIDO / INICIO	El artículo / elementos del artículo son incorrectos	El rendimiento del artículo se degrada.

Tabla 18 Modos de funcionamiento y estado del ítem

7.2.1.5 Restricciones Operacionales

Los ítems se utilizarán únicamente con vehículos en autostrada solo en la región de la UE, no se utilizarán en entorno todoterreno embarrado.

7.2.1.6 Normas Relevantes

Los estándares relevantes con respecto a la funcionalidad y el caso de uso del artículo son:

- Sistemas de asistencia para mantenerse en el carril (LKAS): ISO 11270-2014
- ACC: ISO 15622-2010
- Niveles de automatización: SAE J3016
- Punto ciego: ISO1738

7.2.1.7 Elementos similares

La experiencia y el conocimiento de sistemas relevantes más antiguos y el historial de manejo de funcionalidades similares brindan una ventaja valiosa en el diseño de elementos, por lo que es recomendable recopilar información sobre la funcionalidad y los modos de falla del sistema anterior.

La funcionalidad del artículo es una combinación de ACC, LC, detección de puntos ciegos y reconocimiento de señales de tráfico, no hay experiencia con un artículo similar en la organización como un solo sistema.

Sin embargo, existe un número de elementos individuales que son responsables de algunas de las funciones del elemento de la siguiente manera:

- Control longitudinal: Programa de estabilidad electrónica (ESP) y ACC
- Control lateral: ESP y dirección asistida electrónica (EPS)

7.2.1.8 Modos de Falla y Peligro

Los modos de falla y los peligros se definen en base a la experiencia de un sistema similar, son:

- Modos de fallo
 - El artículo envía información incorrecta a CAN
 - El artículo calcula incorrectamente la distancia y la velocidad del objeto objetivo
 - El artículo detecta incorrectamente la región de punto ciego / señales de tráfico / marcas de carril
- Fallo de HMI

- Peligros

- Aceleración o desaceleración involuntaria
- Pérdida de control de la dirección
- El conductor entra en pánico y frena para cumplir con el límite de velocidad
- El vehículo se desvía del carril objetivo previsto y choca con el tráfico adyacente

7.2.1.9 Interfaces

El artículo enviará una solicitud de aceleración / desaceleración longitudinal, aceleración lateral utilizando par de dirección, señales de advertencia sobre la disponibilidad de puntos ciegos e indicaciones de señales de tráfico en la CAN. El artículo recibirá el estado del modelo de vehículo ego e información de los sensores de percepción sobre el medio ambiente.

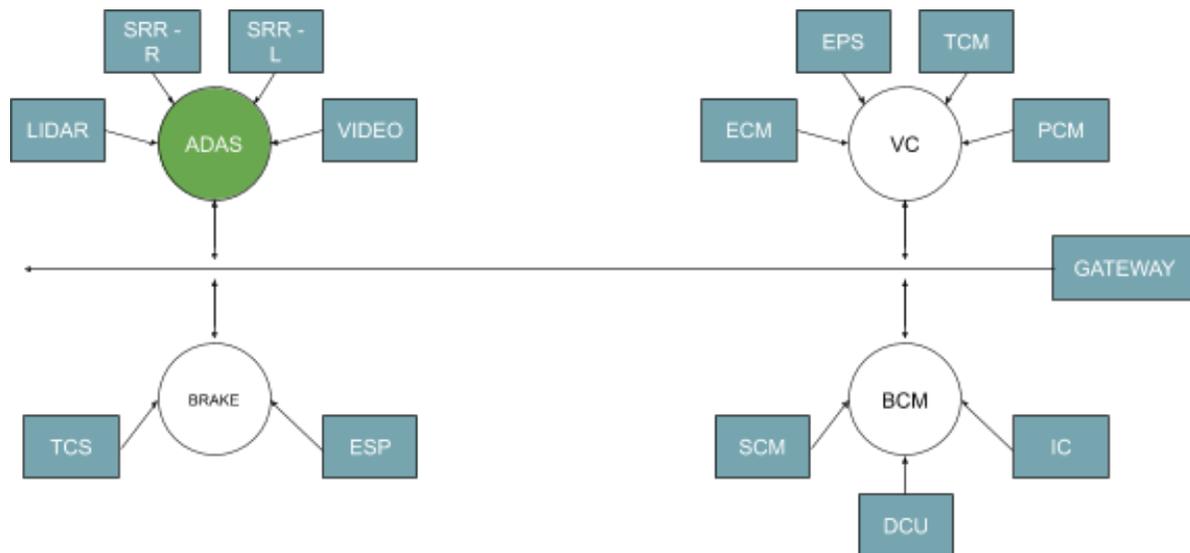


Figura 40 Límite de interacción del elemento

- VC - Control de vehículos
- TCM - Gestión de control de transmisión
- ECM - Gestión de control del motor
- PCM - Gestión de control del tren motriz
- EPS - Dirección asistida electrónica
- ESP - Programa de estabilidad electrónica
- IC - Cluster de instrumentación
- TCS - Sistema de control de tracción

7.2.1.10 Interacciones

El artículo se comunica con otras ECU a través de CAN. El ítem se enciende durante la fase del poder.

7.2.1.11 Interfaz Externa

El ítem se comunica con otros ítems del sistema fuera de su límite con CAN. *La Figura 40* muestra los límites del ítem y otros sistemas. El otro sistema proporciona el estado del vehículo y maneja la funcionalidad requerida por el artículo, a continuación, se muestran los manejados por otros sistemas:

- EPS: el módulo EPS aceptará la solicitud de control de par de dirección y proporcionará información sobre el ángulo de dirección.
- EMS: el sistema del módulo del motor aceptará la solicitud de aceleración
- ESP: El módulo de estabilidad aceptará la solicitud de aceleración y proporcionará la velocidad de la rueda y la velocidad de guiñada.
- HMI: HUD admitirá la visualización de advertencias y alertas
- CAN: Debe transmitir y suministrar información sin latencia ni corrupción de datos
- BCM: el módulo de la carrocería proporcionará la velocidad del vehículo

7.2.1.12 Elementos Funcionales

Los elementos funcionales del ítem se basan en el concepto de asignación de funciones discutido exploración y requisitos del sistema. Son los siguientes:

- 2 SRR: para asistencia de ángulo muerto, ya que solo requiere la información sobre los objetos en el área trasera del vehículo
- 1 Cámara: para seguir las marcas de los carriles, controlar las señales de tráfico y clasificar los tipos de objetos
- 1 LIDAR: para medir la distancia, la velocidad y la asistencia del objeto

El subsistema ADAS es responsable de la fusión de datos del sensor, recopila la información de los objetos de diferentes sensores y forma una estructura de datos con información relevante sobre la velocidad del objeto objetivo, la distancia, el carril del ego y determina la aceleración / desaceleración necesaria, las alertas de HMI y la solicitud de par de dirección.

7.2.1.13 Situación Operativa Común

El elemento está destinado a activarse durante la conducción en carretera, podría involucrar los siguientes escenarios:

- <30 km / h objetivo presente
- > 30 km / h sin objetivo presente
- <50 km / h con marcas de carril
- > 50 km / h con marcas de carril
- > 50 km / h con marcas de carril / sin marcas
- Maniobra de cambio de carril con punto ciego ocupado a todas las velocidades

7.2.2 ANÁLISIS SITUACIONAL E IDENTIFICACIÓN DE PELIGROS

7.2.2.1 Escenarios y Modos Operativos

1. Desvinculación del sistema al tomar curvas o giros cerrados: El sistema se encuentra vinculado a priori al evento, en modo operativo y por las razones mencionadas a continuación el sistema falla y/o se desvincula y esto causa una intervención inmediata a último instante del conductor:

Las líneas límite y de carril se han desvanecido producto al desgaste.

- Las líneas límite y de carril no están bien señalizadas.
- El controlador de movimiento lateral falla.
- Ruido en los sensores.

Se asume que esta acción de intervención a último momento puede provocar que el conductor no reaccione adecuadamente y provoque un peligro mayor o provocar un accidente por una mala maniobra.

Definición de Caso de Uso
Monitorear las líneas del carril y límites de la carretera, así como los vehículos alrededor.
Monitorear la presencia de vehículos en el carril adyacente para ayudar al conductor al centrar el vehículo en el carril
Si el sistema está vinculado, asiste al conductor mediante el control autónomo lateral del EPS
La expectativa es que el conductor responda a las advertencias y permanezca en el carril.
Descripción del caso de uso
El sistema de asistencia al conductor longitudinalmente y LKSA del vehículo se encuentra activado en carreteras con líneas límites visibles y falla al poder concretar la maniobra de curva

satisfactoriamente.
Control del vehículo: el conductor sostiene el volante Estado de funcionalidad: activo Advertencia al conductor: visual y auditiva Usuario de la vía vulnerable: situaciones de tráfico y otros
El vehículo está a punto de tomar una curva, seguir las líneas límites del carril actual. Tipo de camino y descripción: autostrada Estado del tiempo: soleado/noche Acciones de amenaza: Desvinculación del sistema en mitad de la maniobra de curva.
Implementación de casos de uso
Vehículo se encuentra realizando una maniobra para tomar una curva, con vehículos presente en el carril adyacente y/o adelante.
N/A
Lámpara en el HUD
Requisitos Funcionales
N/A
ISO 11270:2014
2020 MCA All rights reserved

Tabla 19 Caso de Uso Desvinculación del sistema al tomar curvas

2. Mal interpretación de líneas de tráfico horizontales. El sistema se encuentra vinculado a priori al evento, en modo operativo. El sistema experimenta el fallo al realizar intento de hacer cambio de carril para continuar la ruta predeterminada. Esta situación provoca que el conductor intervenga de manera inmediata a último instante antes de que se pueda exponer a una situación peligrosa de mayor nivel.

- Sistema no desarrollado para escenarios de carreteras y situaciones inusuales.
- Esta acción de intervención a último momento puede provocar que el conductor no reaccione adecuadamente y provoque un peligro mayor o provocar un accidente por una mala maniobra. El sistema debería de ser capaz de maniobrar de manera segura en circunstancias inusuales y de no ser capaz de realizar la maniobra, alertar con anticipación al conductor.

Definición de Caso de Uso
Monitorear la presencia de Señales de Tráfico Verticales / Horizontales
Monitorear la presencia de señales de tráfico horizontales en ambientes urbanos.
Si el sistema está vinculado, se espera que responda mediante los controladores longitudinales el vehículo.
Se promueve que el conductor responda a las advertencias de señales de tráfico identificadas por el sistema.
Descripción del caso de uso
El vehículo se encuentra en modo activo, con el sistema vinculado, en carreteras con señales de tráfico horizontales, en donde falla al realizar la maniobra para cambiar de carril y seguir la ruta

establecida por el conductor, tiende a tomar el carril (salida) de la izquierda predeterminadamente.
Control del vehículo: El conductor sostiene el volante Estado de funcionalidad: activo Advertencia al conductor: visual y auditiva Usuario de la vía vulnerable: situaciones de tráfico y otros
Qué está pasando: el vehículo está a punto de cambiar de carril y/o alocarse al carril de salida. Tipo de camino y descripción: autostrada Estado del tiempo: soleado / noche Acciones de amenaza: no aplicable
Implementación de casos de uso
Vehículo se encuentra realizando un cambio de carril, sin vehículos en el carril adyacente
N/A
Lámpara en el HUD
Requisitos Funcionales
N/A
ISO 17387:2008
2020 MCA All rights reserved

Tabla 20 Caso de Uso Mal interpretación de líneas de tráfico horizontales

3. Situaciones Climáticas: Nieve - Lluvia - Nublado (Baja visibilidad): El sistema presenta mal funcionamiento en la detección de objetos bajo circunstancias climáticas no aptas y mencionadas a más profundidad a continuación:

- En condiciones de abundante nieve, el sistema no es capaz de localizar e identificar los límites de los carriles vecinos, debido a que una parte de la línea no es visible producto a la nieve, y termina en la intervención humana a último instante, lo que podría provocar una situación peligrosa al no intervenir correctamente.
- En condiciones de abundante lluvia y carreteras con charcos y mantos de lluvia cubriendo las líneas horizontales de la carretera, provoca que el sistema se desvincule y falle al localizar las líneas del carril y termine en la intervención humana a último instante, lo que podría provocar una situación peligrosa al no intervenir correctamente.
- En condiciones de baja visibilidad producto a la neblina, el sistema tiene dificultades en operar por sí mismo y de identificar objetos que se le dificulta categorizar producto a la neblina.
- El sistema debería de ser capaz de operar bajo cualquier condición de baja visibilidad e identificar objetos, categorizarlos y tomar decisiones propias.

Definición de Caso de Uso
Monitorear los señales de tráfico horizontales tales como límites de carril / carretera.
Monitorear la presencia de vehículos en el carril adyacente para ayudar al conductor durante la maniobra de cambio de carril.
Si el carril está ocupado y el conductor está cambiando de carril con o sin luces indicadoras, advierte al conductor sobre una colisión de carril adyacente.
Se evita la colisión lateral, se garantiza la seguridad del tráfico y del conductor; la expectativa es que el conductor responda a las advertencias y permanezca en el carril.
Descripción del caso de uso
Vehículo en distintas circunstancias climáticas, con el sistema activo, se enfrenta a limitaciones de visibilidad y falla al detectar los límites externos de la carretera y aborta al tener baja visibilidad.
Control del vehículo: el conductor sostiene el volante Estado de funcionalidad: activo Advertencia al conductor: visual y auditiva Usuario de la vía vulnerable: situaciones de tráfico y otros
Qué está pasando: el vehículo está a punto de cambiar de carril Tipo de camino y descripción: autostrada Estado del tiempo: nieve / lluvia / neblina Acciones de amenaza: no aplicable
Implementación de casos de uso
Vehículo se encuentra en carretera, utilizando LKSA para centrarse en el carril.
N/A
Lámpara en el HUD

Requisitos Funcionales
N/A
ISO 21717: 2018
2020 MCA All rights reserved

Tabla 21 Caso de Uso Situaciones Climáticas

4. Ambientes Urbanos: El sistema no es capaz de desarrollar maniobras usuales en ambientes urbanos, la toma de decisión está basada en la imagen formada por fusión de los sensores. Se analizará más a fondo los distintos escenarios donde el sistema falla o experimenta un mal funcionamiento.

- El identificar señales de tráfico es una característica que muchos vehículos poseen hoy en día, el poder tomar una decisión en base a la combinación de factores que rodea al vehículo y ajustar constantemente todo el rango de operaciones mecánicas en un ambiente urbano, es una meta. Entre más kilómetros recorridos tenga los vehículos de prueba, más información podrán captar de eventos en escenarios reales e inusuales y es este tipo de datos que ayudan a mejorar el sistema a tomar decisiones en escenarios urbanos, semáforos, intersecciones, rotondas, rastreo constante de objetos múltiples, etc.
- El sistema experimenta fallas al localizar efectivamente la línea de pare y los límites de las intersecciones no marcadas o pocas visibles.
- No es capaz de realizar maniobras en calles con vehículos parqueados sobre el carril y no se identifica una maniobra para maniobrar alrededor de los vehículos parqueados en el carril.

Definición de Caso de Uso
Monitorear la presencia de vehículos en el carril adyacente
Monitorear la presencia de vehículos en el carril adyacente para ayudar al conductor durante la maniobra de cambio de carril.
Si el carril está ocupado y el conductor está cambiando de carril con o sin luces indicadoras, advierta al conductor sobre una colisión de carril adyacente.
Monitorear la presencia de señales de tráfico horizontal y vertical. Advertir al conductor sobre señales de tráfico identificadas, así como de una colisión por maniobra de giro o al detectar un objeto en la proyección determinada.
Descripción del caso de uso
Vehículo con estado activo del sistema de asistencia al conductor circulando por ambientes urbanos
Control del vehículo: el conductor sostiene el volante Estado de funcionalidad: activo Advertencia al conductor: visual y auditiva Usuario de la vía vulnerable: situaciones de tráfico urbano
Qué está pasando: el vehículo circula por varias situaciones en ambientes urbanos. Tipo de camino y descripción: autostrada Estado del tiempo: soleado / nublado Acciones de amenaza: no aplicable
Implementación de casos de uso
Vehículo se encuentra realizando maniobras en ambientes urbanos
N/A
Lámpara en el HUD

Requisitos Funcionales
N/A
ISO 17287:2019
2020 MCA All rights reserved

Tabla 22 Caso de Uso Ambientes Urbanos

7.2.3 HAZOP

7.2.3.1 Eventos Peligrosos

Desvinculación del sistema al tomar curvas

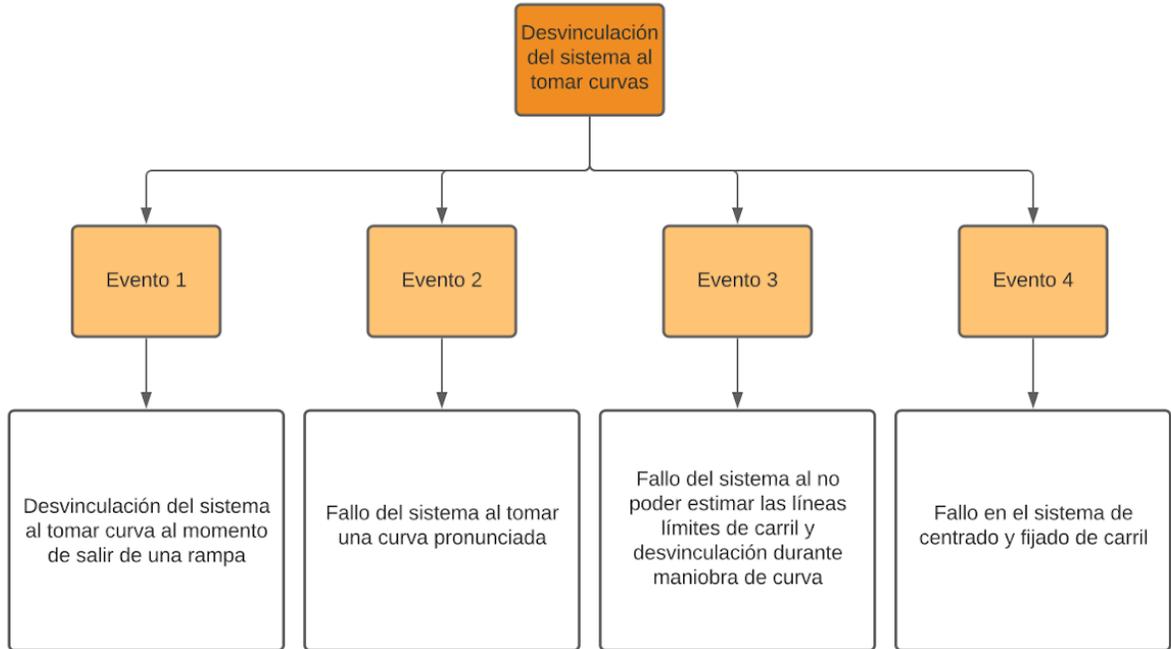


Figura 41 Eventos Peligrosos - Desvinculación en Curva

Falla de detección de señales horizontales y de múltiples objetos

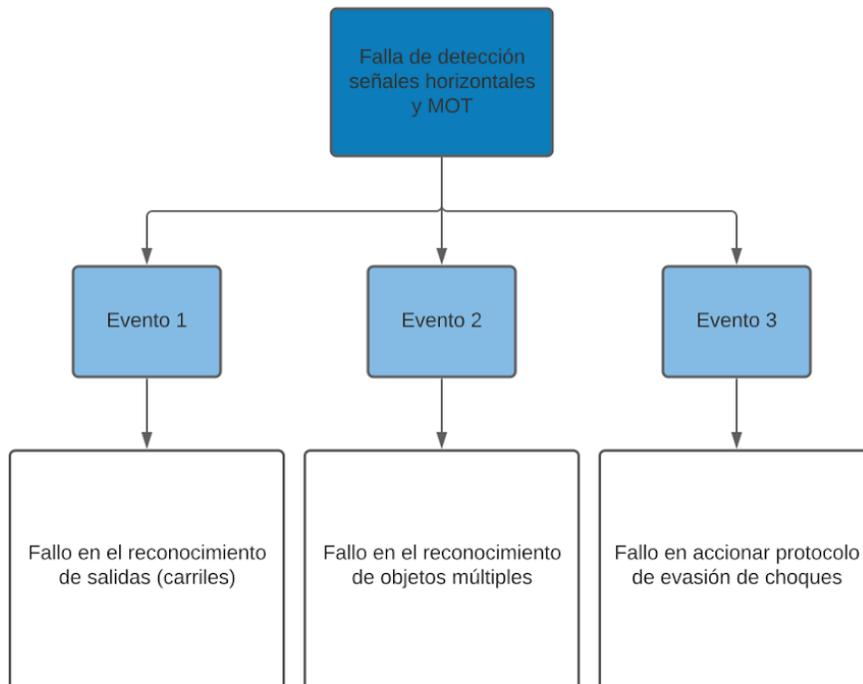


Figura 42 Eventos Peligrosos - Detección de Señales Horizontales y Múltiples Objetos

Situaciones Climáticas

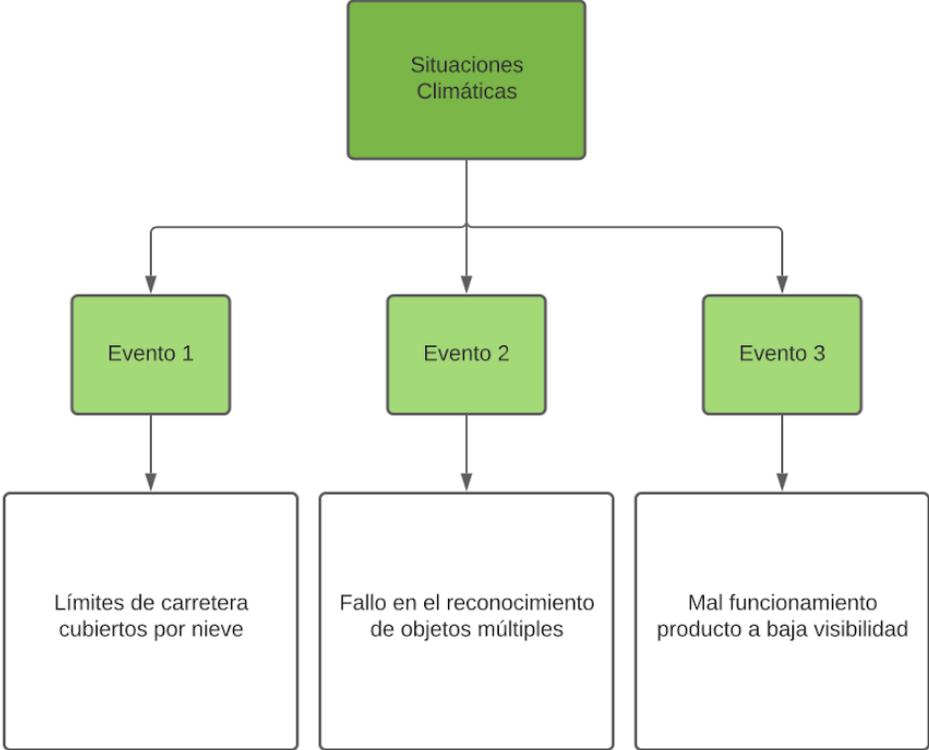


Figura 43 Eventos Peligrosos - Situaciones Climáticas

Ambientes Urbanos

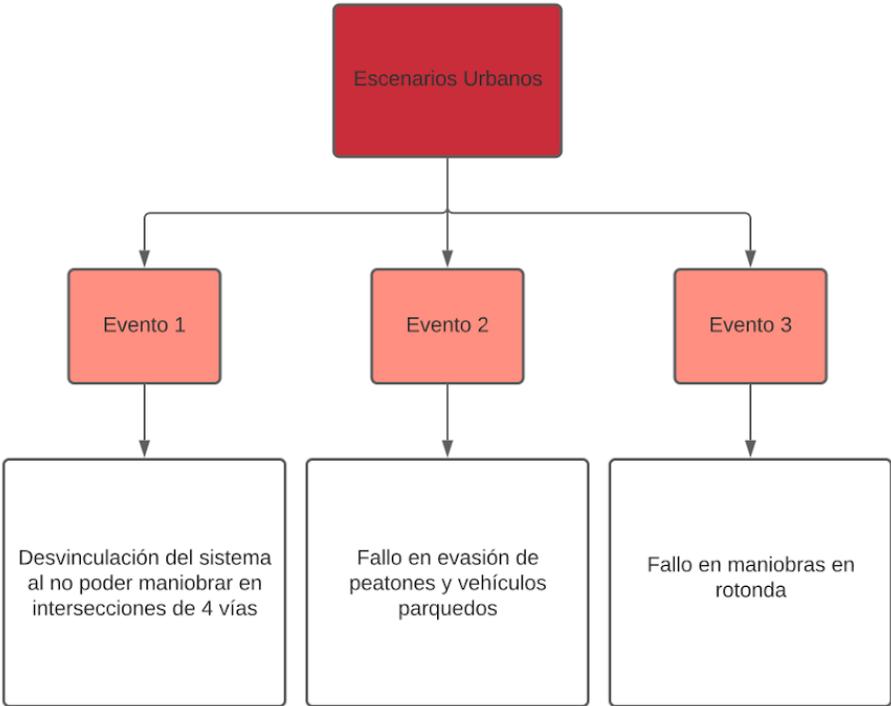


Figura 44 Eventos Peligrosos - Escenarios Urbanos

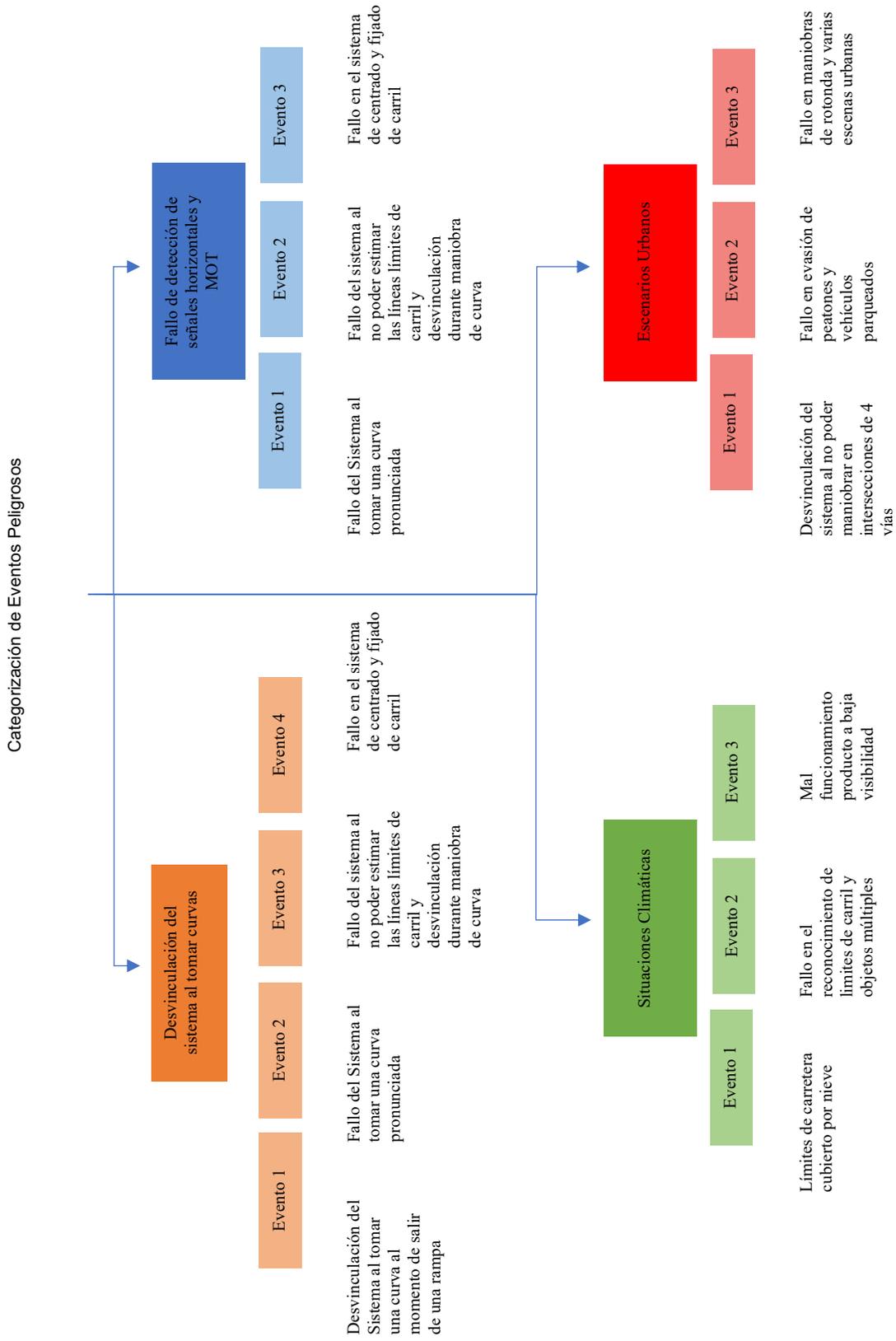


Figura 45 Resumen de Eventos Peligrosos

7.2.3.1 Parametrización de S, E y C

En esta sección, se clasifican los eventos peligrosos, basados en las métricas: Severidad, Exposición y Controlabilidad presentadas en las *Tablas 10 – 12*.

7.2.3.1.1 Severidad

CLASE	S0	S1	S2	S3
Descripción	No existe lesiones	Lesiones Ligeras / Moderadas	Lesiones graves y potencialmente mortal (supervivencia probable)	Lesiones potencialmente mortales (supervivencia incierta)

Tabla 23 Parametrización de Severidad, Bluvband & Grabov (2009)

Desvinculación del sistema al tomar curvas o giros cerrados

Evento 1

CLASE	S0	S1	S2	S3
-------	----	----	----	----

Evento 2

CLASE	S0	S1	S2	S3
-------	----	----	----	----

Evento 3

CLASE	S0	S1	S2	S3
-------	----	----	----	----

Evento 4

CLASE	S0	S1	S2	S3
-------	----	----	----	----

Falla de detección de señales horizontales y de múltiples objetos

Evento 1

CLASE	S0	S1	S2	S3
-------	----	----	----	----

Evento 2

CLASE	S0	S1	S2	S3
-------	----	----	----	----

Evento 3

CLASE	S0	S1	S2	S3
-------	----	----	----	----

Situaciones Climáticas

Evento 1

CLASE	S0	S1	S2	S3
-------	----	----	----	----

Evento 2

CLASE	S0	S1	S2	S3
-------	----	----	----	----

Evento 3

CLASE	S0	S1	S2	S3
-------	----	----	----	----

Ambientes Urbanos

Evento 1

CLASE	S0	S1	S2	S3
-------	----	----	----	----

Evento 2

CLASE	S0	S1	S2	S3
-------	----	----	----	----

Evento 3

CLASE	S0	S1	S2	S3
-------	----	----	----	----

7.2.3.1.2 Exposición

CLASE	E0	E1	E2	E3	E4
Descripción	Increíble	Probabilidad muy baja	Probabilidad Baja	Probabilidad Mediana	Probabilidad Alta

Tabla 24 Parametrización de Exposición, Bluvband & Grabov (2009)

Desvinculación del sistema al tomar curvas o giros cerrados

Evento 1

CLASE	E1	E2	E3	E4
-------	----	----	----	----

Evento 2

CLASE	E1	E2	E3	E4
-------	----	----	----	----

Evento 3

CLASE	E1	E2	E3	E4
-------	----	----	----	----

Evento 4

CLASE	E1	E2	E3	E4
-------	----	----	----	----

Falla de detección de señales horizontales y de múltiples objetos

Evento 1

CLASE	E1	E2	E3	E4
-------	----	----	----	----

Evento 2

CLASE	E1	E2	E3	E4
-------	----	----	----	----

Evento 3

CLASE	E1	E2	E3	E4
-------	----	----	----	----

Situaciones Climáticas

Evento 1

CLASE	E1	E2	E3	E4
-------	----	----	----	----

Evento 2

CLASE	E1	E2	E3	E4
-------	----	----	----	----

Evento 3

CLASE	E1	E2	E3	E4
-------	----	----	----	----

Ambientes Urbanos

Evento 1

CLASE	E1	E2	E3	E4
-------	----	----	----	----

Evento 2

CLASE	E1	E2	E3	E4
-------	----	----	----	----

Evento 3

CLASE	E1	E2	E3	E4
-------	----	----	----	----

7.2.3.1.3 Controlabilidad

Descripción	Controlable en general	Simplemente controlable	Normalmente controlable	Difícil de Controlar - Incontrolable
-------------	------------------------	-------------------------	-------------------------	--------------------------------------

Tabla 25 Parametrización de Controlabilidad, Bluvband & Grabov (2009)

Desvinculación del sistema al tomar curvas o giros cerrados

Evento 1

CLASE	C0	C1	C2	C3
-------	----	----	----	----

Evento 2

CLASE	C0	C1	C2	C3
-------	----	----	----	----

Evento 3

CLASE	C0	C1	C2	C3
-------	----	----	----	----

Evento 4

CLASE	C0	C1	C2	C3
-------	----	----	----	----

Falla de detección de señales horizontales y de múltiples objetos

Evento 1

CLASE	C0	C1	C2	C3
-------	----	----	----	----

Evento 2

CLASE	C0	C1	C2	C3
-------	----	----	----	----

Evento 3

CLASE	C0	C1	C2	C3
-------	----	----	----	----

Situaciones Climáticas

Evento 1

CLASE	C0	C1	C2	C3
-------	----	----	----	----

Evento 2

CLASE	C0	C1	C2	C3
-------	----	----	----	----

Evento 3

CLASE	C0	C1	C2	C3
-------	----	----	----	----

Ambientes Urbanos

Evento 1

CLASE	C0	C1	C2	C3
-------	----	----	----	----

Evento 2

CLASE	C0	C1	C2	C3
-------	----	----	----	----

Evento 3

CLASE	C0	C1	C2	C3
-------	----	----	----	----

7.2.4 CLASIFICACIÓN DE EVENTOS PELIGROSOS

A continuación, se presenta la asociación de ASIL para cada uno de los eventos analizados anteriormente. El nivel de ASIL será utilizado para desarrollar los objetivos de seguridad en los siguientes apartados.

Severity	Exposure	Controllability		
S	E	C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Tabla 26 ASIL Categorización de Eventos Peligrosos, ISO 26262 (2011)

7.2.4.1 Desvinculación del sistema al tomar curvas o giros cerrados

Severity	Exposure	Controllability		
		C1	C2	C3
S	E	C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Tabla 27 ASIL Desvinculación del sistema al tomar curvas o giros

- Evento 1 (Azul): Desvinculación del sistema al tomar curva al momento de salir de una rampa.
- Evento 2 (Rojo): Fallo del sistema al tomar una curva cerrada.
- Evento 3 (Anaranjado): Fallo del sistema al no poder estimar las líneas límites de carril y desvinculación del sistema durante maniobra de curva.
- Evento 4 (Verde): Fallo en el sistema de centrado y fijado de carril.

7.2.4.2 Falla de detección de señales horizontales y de múltiples objetos

Severity	Exposure	Controllability		
S	E	C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Tabla 28 ASIL Falla de detección de señales horizontales y de múltiples objetos

Evento 1 (Azul): Fallo en el reconocimiento de carriles (salidas)

Evento 2 (Rojo): Fallo en el reconocimiento de objetos

Evento 3 (Anaranjado): Fallo en accionar protocolo de evasión de choques

7.2.4.3 Situaciones Climáticas

Severity	Exposure	Controllability		
S	E	C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Tabla 29 ASIL Situaciones Climáticas

Evento 1 (Azul): Límites de carretera cubierto por nieve

Evento 2 (Rojo): Límites de carretera cubierto por mantos acuíferos

Evento 3 (Anaranjado): Baja Visibilidad provocado por neblina

7.2.4.4 Ambientes Urbanos

Severity	Exposure	Controllability		
		C1	C2	C3
S	E	C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Tabla 30 ASIL Ambiente Urbano

Evento 1 (Azul): Intersecciones de 4 vías

Evento 2 (Rojo): Fallo en evasión de peatones y objetos parqueados

Evento 3 (Anaranjado): Fallo en maniobras usuales (varias)

7.2.5 DETERMINACIÓN DE OBJETIVOS DE SEGURIDAD

ISO 26262 ha establecido que para cada uno de los eventos peligrosos e ítems se tiene que desarrollar un objetivo de seguridad. A continuación se enlistan los ítems y se determinan los objetivos de seguridad para cada uno. Estos objetivos de seguridad son el resultado del análisis de riesgo y determinación de ASIL. El enfoque será únicamente aquellos eventos que tienen un nivel de ASIL distinto de QM, es decir que posean un resultado A, B, C o D, siendo D el nivel con mayor riesgo mostrados en la *tabla 19*.

7.2.5.1 Desvinculación del sistema al tomar curvas o giros cerrados

#	Eventos	Objetivos de Seguridad
1	Desvinculación del sistema al tomar una curva al momento de salir de una rampa.	<p>El sistema deberá controlar el EPS y el sistema de comunicación (GPS), en conjunto con la información de los distintos ECU's. Identificar el carril adecuado para la continuación de la ruta predeterminada y/o ajustar mediante el controlador de cambio de carril.</p> <p>En el caso que el sistema no pueda ejecutar la maniobra, notificar al conductor y transferir controles al conductor sin desvincular el sistema hasta entonces.</p> <p>FFTI > 5 Segundos</p>
2	Fallo en el sistema al tomar una curva pronunciada	<p>El sistema deberá controlar el EPS en todas circunstancias, cuando el sistema este activado, incluso en curvas pronunciadas si el sistema no detecte riesgos externos.</p> <p>FFTI > 4 segundos</p>

3	Fallo del sistema al no poder estimar las líneas límites de carril y desvinculación durante maniobra de curva	<p>El sistema deberá de proyectar los límites de las líneas de carril mediante realidad aumentada, en el caso que se vean obstruidas.</p> <p>En el caso que el sistema no pueda realizar la maniobra, notificar al conductor y no desvincular el sistema hasta que el conductor tome control, para que exista una transferencia de controles regulados y con menor riesgo de intervención.</p> <p style="text-align: center;">FTTI > 6 segundos</p>
4	Fallo en el sistema de centrado y fijado de carril	<p>El sistema deberá proyectar los límites de las líneas de carril mediante realidad aumentada, en el caso que se vean obstruidas.</p> <p>Mediante el controlado LKPAS centrar el vehículo en medio del carril, de no ser posible no permitir la activación del sistema a priori. Ni durante operación si el sistema no es capaz de detectar los límites de carril.</p> <p style="text-align: center;">FTTI > 5 segundos</p>

Tabla 31 Objetivos de Seguridad: Desvinculación del sistema al tomar curvas

7.2.5.2 Fallo de detección de señales horizontales y MOT

#	Eventos	Objetivos de Seguridad
1	Fallo en el reconocimiento de salidas (carriles)	<p>El sistema deberá identificar las salidas mediante los sensores de camera en conjunto con los sistemas de comunicación y localización del vehículo (GPS), y poder ajustar la velocidad y maniobrar el EPS y poder continuar la ruta pre determinada por el usuario.</p> <p>En el caso que el sistema falle, deberá de reconocer el error y notificar al conductor del tal para que exista una transferencia de mando seguro. El sistema deberá permanecer vinculado hasta que el conductor tome control del timón.</p> <p style="text-align: center;">FTTI > 6 - 8 segundos</p>
2	Fallo en el reconocimiento de objetos múltiples.	<p>El sistema deberá identificar, detectar y clasificar distintos objetos, y poder categorizarlos. Así como darle seguimiento y calcular un estimado del posicionamiento de objetos movibles en los siguientes segundos y accionar los controladores longitudinales (velocidad y distancias) y laterales (EPS).</p> <p>Si existe una situación de colisión activar el sistema de aviso de colisión y protocolo de evasión de colisión.</p> <p>El sistema deberá permanecer vinculado en todo</p>

		<p>el momento hasta después de realizar la maniobra de evasión.</p> <p>FTTI > Post maniobra + 2 segundos</p>
3	Fallo en accionar protocolo de choques	<p>El sistema deberá detectar posibles colisiones del vehículo con otros objetos y viceversa y deberá activar automáticamente el protocolo de evasión de colisión.</p> <p>El sistema debe tener un mecanismo de redundancia ante cualquier anomalía. En el caso de fallo de la función, el sistema deberá notificar la falla y solicitar de inmediato la intervención del conductor, tomando en cuenta el tiempo de reacción (TFFI) promedio de un conductor 3 – segundos</p> <p>TFFI > +3 Segundos</p>

Tabla 32 Objetivos de Seguridad: Fallo de detección de señales horizontales y MOT

7.2.5.3 Situaciones Climáticas

#	Eventos	Objetivos de Seguridad
1	Límites de carretera cubierto por nieve	<p>El sistema deberá de proyectar los límites de las líneas de carril mediante realidad aumentada, en el caso que se vean obstruidas.</p> <p>En el caso que el sistema no pueda maniobrar el vehículo, notificar al conductor y no desvincular el sistema hasta que el conductor tome control, manteniendo el vehículo centrado en el carril, para que exista una transferencia de controles regulado y con menor riesgo de intervención.</p> <p>FTTI > 6 segundos</p>
2	Fallo en el reconocimiento de objetos múltiples	<p>El sistema deberá identificar, detectar y clasificar objetos. Así como darle seguimiento y calcular un estimado del posicionamiento de objetos movibles en los siguientes segundos y accionar los controladores longitudinales (velocidad y distancias) y laterales (EPS).</p> <p>El sistema deberá permanecer vinculado en todo el momento. Si el sistema falla en identificar y clasificar el objeto, el sistema deberá categorizarlo como “objeto no identificado”, el sistema deberá maniobrar y evadir el objeto, si es necesario.</p>

		<p>En caso de falla, el sistema deberá alertar al conductor para que tome control del vehículo, deberá existir una transferencia de controles regulado y con el menor riesgo dado por la intervención humana</p> <p>FTTI > Post maniobra + 2 segundos</p>
3	Mal Funcionamiento producto a baja visibilidad	<p>El sistema deberá proyectar los límites de las líneas de carril mediante realidad aumentada, en el caso que se vean obstruidas o que los sensores de video se les dificulte detectar las señales horizontales / verticales producto a la baja visibilidad.</p> <p>En el caso que el sistema aborte producto a falla deberá notificar al conductor y mantenerse vinculado centrando el vehículo en el carril, hasta que el conductor tome control del vehículo para que exista una transferencia de controles regulado y con menor riesgo de intervención.</p> <p>FTTI > 4 segundos</p>

Tabla 33 Objetivos de Seguridad: Situaciones Climáticas

7.2.5.4 Ambientes Urbanos

#	Eventos	Objetivos de Seguridad
1	Intersecciones de 4 via	<p>El Sistema deberá identificar las líneas de pare, de lo contrario proyectar una línea de pare en base a las proyecciones de realidad aumentada. El identificar señales de tráfico (semáforos, señales verticales y horizontales) y vehículos en los carriles adyacentes, así como otros objetos interactuando en la intersección.</p> <p>En el caso que el vehículo llegue a la intersección y el semáforo se encuentre en verde y exista un vehículo delante que sirva como guía (siempre que la ruta del vehículo coincida con la ruta determinada) el sistema seguirá el vehículo sin necesidad de confirmación del conductor para realizar la maniobra.</p> <p>En el caso que no exista un semáforo que regule el flujo de tráfico. El sistema deberá detectar los vehículos que llegan de primero a la intersección y respetar el orden de llegada de los vehículos, y posicionarse en la línea de pare y esperar la confirmación del conductor para realizar la maniobra de cruce.</p> <p>En el caso que no se encuentren otros vehículos en la intersección, el sistema igual tendrá que detenerse en la línea de pare y esperar la confirmación de la maniobra de parte del conductor.</p> <p style="text-align: center;">FTTI > 2 Segundos</p>

2	Fallo en evasión de peatones y objetos parqueado	<p>El sistema deberá identificar, detectar y clasificar distintos objetos, y poder categorizarlos. Así como darle seguimiento y calcular un estimado del posicionamiento de objetos movibles en los siguientes segundos y accionar los controladores longitudinales (velocidad y distancia) y laterales (EPS).</p> <p>El sistema deberá permanecer vinculado en todo momento, Si el sistema falla en identificar y clasificar el objeto, el sistema deberá detectarlo y categorizarlo como “objeto no identificado”, el sistema deberá maniobrar y evadir el objeto.</p> <p style="text-align: center;">FTTI > 2 Segundos</p>
3	Fallo en maniobras de rotonda (varias)	<p>El sistema deberá disminuir la velocidad antes de llegar a la línea de pare en la rotonda así como situar al vehículo en el carril que corresponde para continuar la ruta. El sistema deberá analizar el resto de los vehículos a su alrededor (carriles adyacentes y carriles dentro de la rotonda) y objetos.</p> <p>En el caso que exista una ventana para realizar la maniobra de entrada en la rotonda, deberá de notificar al conductor cuando el sistema detecte que existe una ventana de oportunidad que no implique un riesgo mayor a QM, y el conductor deberá de aceptar / rechazar la operación. En el caso que la operación se aceptada por el conductor, el sistema tendrá que realizar la maniobra y detectar el carril que corresponde entrar, en base a la ruta pre determinada por el usuario.</p>

		<p>En el caso que el sistema falle en identificar la ventana de oportunidad para realizar esta maniobra, deberá de desvincular el sistema una vez se encuentre el vehículo detenido en la línea de pare (antes de entrar a los carriles internos de la rotonda). El sistema deberá mantenerse vinculado centrando el vehículo en el carril hasta llegar a la línea de pare de la rotonda y hasta que el conductor tome control del vehículo para que exista una transferencia de controles regulado y con menor riesgo de intervención.</p> <p style="text-align: center;">FTTI > 4 Segundos</p>
--	--	---

Tabla 34 Objetivos de Seguridad: Ambientes Urbanos

7.2.6 REQUISITOS DE SEGURIDAD FUNCIONAL

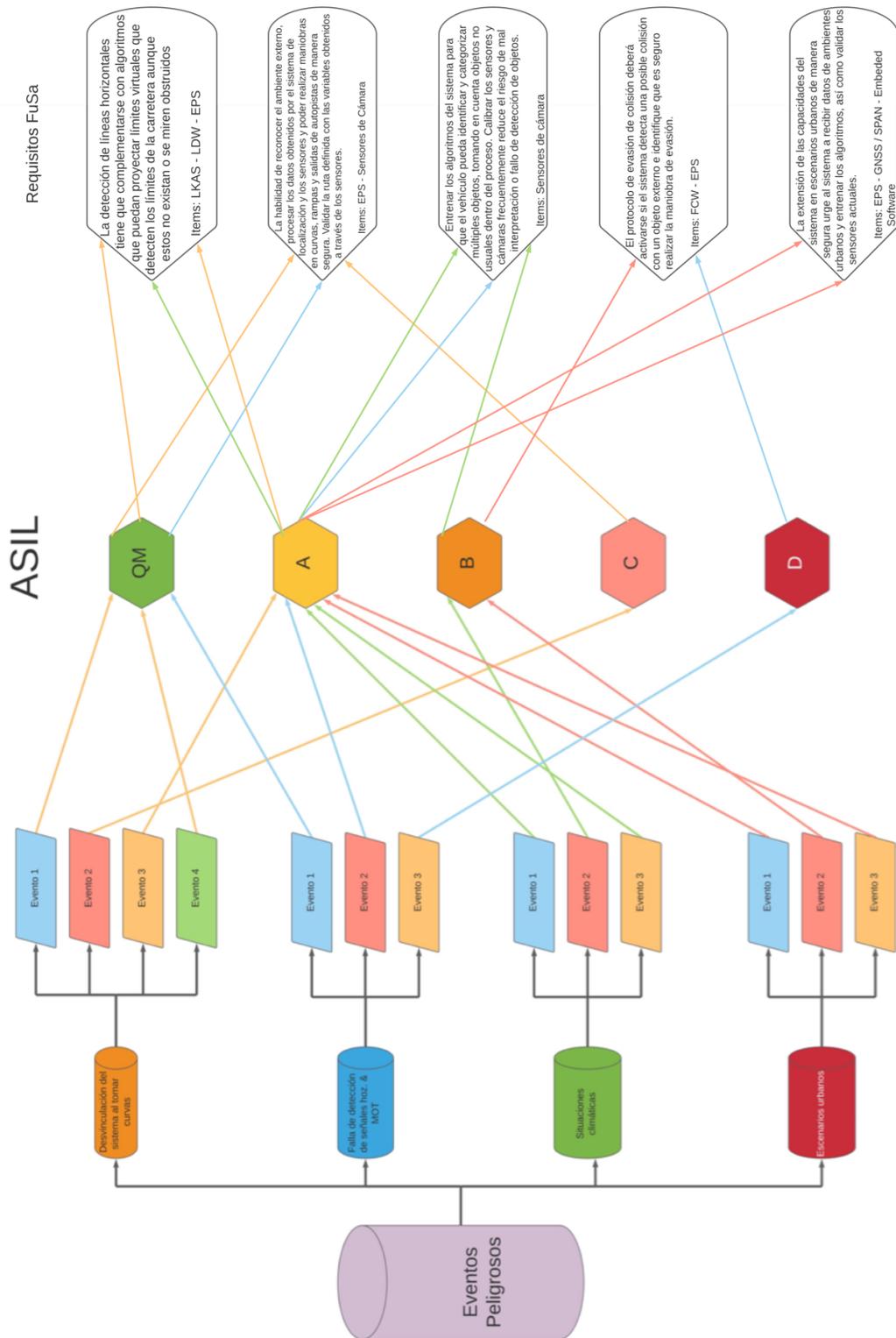


Figura 46 Relación de Ítems con Requisites de Seguridad Funcional

8. CONCLUSIONES

En la presente investigación, se ha analizado el nivel de seguridad del sistema avanzado de asistencia al conductor en vehículos Volvo series 2020 – 2021. Se ha identificado y categorizado los distintos tipos de fallas que limitan la operatividad efectiva del sistema, en donde se considera la intervención del humano (conductor) con el interfaz del sistema. De cara a futuras innovaciones, es evidente que para los niveles de autonomía inferiores (2 – 3), el conductor del vehículo deberá, en todas las circunstancias, tener el vehículo bajo control para poder ejercer monitoreo activo y de ser necesario intervenir, deberá estar en todo momento en condiciones de realizar todas las maniobras requeridas.

La evaluación de las fallas identificadas mediante el desarrollo de un análisis FMEA, permitió la identificación de las causas, modos de fallos y efectos. Dicha evaluación se basó en los criterios de gravedad – frecuencia – detectabilidad de la falla. El promedio del valor de estas tres métricas resultó en el número promedio de riesgo (NPR). El resultado de NPR del estado actual de las fallas sirve como marco de referencia para comparar el puntaje obtenido luego de haber implementado las acciones correctoras propuestas para cada falla. Este análisis dio como resultado la identificación de la cadena de fallo y posibles acciones para mitigar la falla a nivel de sistema, y brinda un mejor entendimiento de la intervención del conductor y el interfaz del vehículo, así como su tiempo de reacción FTTI, analizado posteriormente.

El malfuncionamiento de componentes del sistema conduce a fallas que conducen a un escenario peligroso. Se identificaron mediante el análisis HAZOP, distintos escenarios peligrosos y se evaluó el riesgo de cada uno mediante la determinación de los parámetros: Severidad – Exposición – Controlabilidad. El resultado de la parametrización nos revela el nivel de seguridad integral automotriz ASIL. Exponiendo las futuras capacidades del sistema para los eventos inusuales, analizados en esta investigación.

Finalmente, mediante la aplicación de ambos análisis se concluye con la obtención de objetivos de seguridad basados en razonamientos y datos científicos. Dichos objetivos de seguridad son traducidos en la etapa de desarrollo en requisitos de seguridad funcional.

9. RECOMENDACIONES

La capacidad de control del vehículo ha sido la esencia misma de la conducción de un automóvil; a partir de los requisitos del sistema, es evidente que la capacidad de control del vehículo no está disponible con el conductor todo el tiempo. Esta contradicción debe abordarse con un sistema confiable para niveles más altos de automatización. La metodología perfeccionada con el diseño del sistema y el ciclo de vida de seguridad en la *Figura 37* y la *Figura 38* con pautas adicionales e inclusión de la técnica aplicada en esta investigación: FMEA - HARA, brindan un marco de referencia para poder definir las limitaciones y requisitos de seguridad del sistema, pero no en su totalidad.

La reducción de riesgos que se garantiza a través de objetivos de seguridad y su respectivo concepto de seguridad funcional asistido por medidas externas y la adición de un nuevo canal CAN es un punto de partida para comprender la complejidad en el diseño y los recursos necesarios en un futuro autónomo seguro.

Una de las grandes limitaciones para OEM's en vías de desarrollo de sistemas autónomos de niveles superiores, incluyendo a Volvo, es la falta de estándares y regulaciones que establezca parámetros de operatividad y seguridad. Si bien ISO 26262 sirve como un marco de referencia, es un estándar enfocado para fallas a nivel de componentes E / E, lo cual limita la extensión de poder regular a vehículos con niveles de autonomía superior.

Se recomienda agrupar todos los estándares que existan actualmente, analizar los componentes y ocupar el marco de referencia de tal estándar a nivel de componente. La curva de desarrollo apunta que para que niveles de autonomía alto puedan emerger en los mercados actuales, se necesita una transición segura de las capacidades de niveles inferiores a los niveles altos.

El aseguramiento de **las** capacidades inferiores bajo los marcos de referencia para cada nivel, es una estrategia que agrega valor al desarrollo de niveles de autonomía altos y fomenta las regulaciones federales para cada uno de los niveles, así como el desarrollo de estos sistemas a lo largo de la industria automotriz. La metodología utilizada en el presente trabajo monográfico, podría utilizarse para analizar otros productos de trabajo de la Parte 3 y otras partes de ISO26262 (2018), con el fin de detectar posibles fallas y riesgos nuevos, expandiendo constantemente las capacidades del sistema y funciones. m

REFERENCIAS BIBLIOGRÁFICAS

- ASQ. (2015). Failure Mode & Effects Analysis | ASQ. Retrieved August 12, 2020, from Asq.org website: <https://asq.org/quality-resources/fmea>
- Auto Vision News. (2020, July 15). "Rear Cross-Traffic Alert" Definition & Meaning | AutoVision Glossary. Retrieved September 24, 2020, from AutoVision News website: <https://www.autovision-news.com/glossary/rear-cross-traffic-alert/>
- Brady, D. (2020, July 28). What Is Hill-Descent Control? How Does It Work? Retrieved September 28, 2020, from MotorTrend website: <https://www.motortrend.com/news/hill-descent-control-explained/>
- Brooke, L. (2020). Thermal imaging makes its case for ADAS, AVs. Retrieved July 28, 2020, from Sae.org website: <https://www.sae.org/news/2020/01/thermal-imaging-for-adas-avs>
- Carsten, O., & Nilsson, L. (2001, November). Safety Assessment of Driver Assistance Systems. Retrieved October 31, 2020, from ResearchGate website: https://www.researchgate.net/publication/33038821_Safety_Assessment_of_Driver_Assistance_Systems
- Dubey, A. (2020). Stereo vision- Facing the challenges and seeing the opportunities for ADAS applications. In *Texas Instruments*. Retrieved from https://www.ti.com/lit/wp/spry300a/spry300a.pdf?ts=1601278756585&ref_url=https%253A%252F%252Fwww.google.com%252F
- Duke Science & Society. (2018, April 23). Science Module: Advanced Driver Assistance Systems (ADAS). Retrieved September 28, 2020, from SciPol website: <http://sciencepolicy.duke.edu/content/science-module-advanced-driver-assistance-systems-adas>
- Elliott, M. (2015). ADAS added to automotive electronics website. Retrieved September 23, 2020, from Electronicspecifier.com website: <https://www.electronicspecifier.com/news/analysis/adas-added-to-automotive-electronics-website>

- EU COMMISSION FOR MOBILITY AND TRANSPORT. (2016, October 17). Intelligent speed adaptation. Retrieved September 28, 2020, from European Commission website:
https://ec.europa.eu/transport/road_safety/specialist/knowledge/speed/new_technologies_new_opportunities/intelligent_speed_adaptation_isa_en
- Fleyeh, H. (2008). *Traffic and Road Sign Recognition*. Retrieved from <https://www.diva-portal.org/smash/get/diva2:523372/fulltext01.pdf>
- Hoover, R. L., Rao, S. J., Howe, G., & Barickman, F. S. (2014, November). Vehicle lane departure warning. Retrieved August 26, 2020, from Nhtsa website:
https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/812078_heavy-vehiclelanedepartwarntestdevelmt.pdf
- ISO 7000:2045. (2004). ISO 7000:2045 Traction control. Retrieved September 23, 2020, from Iso.org website: <https://www.iso.org/obp/ui#iso:grs:7000:2048>
- ISO 26262. (2011). ISO 26262-1:2011. Retrieved September 23, 2020, from ISO website: <https://www.iso.org/standard/43464.html>
- Jitesh, S. (2014, October). ANTILOCK BRAKING SYSTEM (ABS). Retrieved September 23, 2020, from ResearchGate website:
https://www.researchgate.net/publication/289251560_ANTILOCK_BRAKING_SYSTEM_ABS
- John, V., & Mita, S. (2017). Deep Sensor Fusion for ADAS Applications. In *Nvidia*. Retrieved from <https://www.nvidia.com/content/apac/gtc/ja/pdf/2018/1033.pdf>
- K.R.K. Sastry, D. S. P. (2015). Automatic Driver Assistance System - Glare Free High Beam Control. *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, 04(07), 5986–5990.
<https://doi.org/10.15662/ijareeie.2015.0407024>
- LJUNG AUST, M. (2012). *Improving the Evaluation Process for Active Safety Functions Addressing Key Challenges in Functional Formative Evaluation of Advanced Driver Assistance Systems*. Retrieved from <http://publications.lib.chalmers.se/records/fulltext/155871.pdf>

- Lundin, A. (2017, February 14). State-of-the-Art Fleet Technology: Safety. Retrieved September 23, 2020, from Automotive-fleet.com website:
<https://www.automotive-fleet.com/157229/state-of-the-art-fleet-technology-safety>
- Mollick, P. (2010, April 15). Automotive Night Vision Systems – Status and Development Trends. Retrieved September 28, 2020, from ResearchGate website:
https://www.researchgate.net/publication/281005005_Automotive_Night_Vision_Systems_-_Status_and_Development_Trends
- Munster, G. (2018, April 3). Seeing the Road Ahead: The Importance of Cameras to Self-Driving Vehicles | Loup Ventures. Retrieved September 28, 2020, from Loup Ventures website: <https://loupventures.com/seeing-the-road-ahead-the-importance-of-cameras-to-self-driving-vehicles-2/>
- NEOPLAN. (2020). Turn assist with active driver warning and pedestrian detection | NEOPLAN. Retrieved September 24, 2020, from Neoplan.com website:
<https://www.neoplan.com/global/en/coaches/technology/safety-and-driver-assistance-systems/turn-assist-with-pedestrian-detection/Turn-assist-with-pedestrian-detection.html>
- NHTSA. (2014, July). Blind spot monitoring in light vehicles system performance. Retrieved August 6, 2020, from Nhtsa website:
file:///Users/adiacaguilar/Downloads/812045_Blind-Spot-Monitoring-in-Light-Vehicles-System-Performance.pdf
- NHTSA. (2015). *Crash Stats: Critical Reasons for Crashes Investigated in the National Motor Vehicle Crash Causation Survey*. Retrieved from
<https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812115>
- NHTSA. (2017, September 7). NHTSA. Retrieved September 23, 2020, from NHTSA website: <https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety>
- NHTSA. (2020). Electronic Stability Control. Retrieved September 23, 2020, from Safercar.gov website: <https://www.safercar.gov/Vehicle-Shoppers/Rollover/Electronic-Stability-Control>
- Pananurak, W., Thanok, S., & Parnichkun, M. (2009, March 25). Adaptive cruise control for an intelligent vehicle. Retrieved September 23, 2020, from ResearchGate website:

https://www.researchgate.net/publication/224441630_Adaptive_Cruise_Control_or_an_Intelligent_Vehicle

Parker, M. (2017). Automotive Radar - an overview. Retrieved July 24, 2020, from Sciencedirect.com website:

<https://www.sciencedirect.com/topics/engineering/automotive-radar>

Pellkofer, A., Rotti, J., & KO, D. (2020). Electric Vehicle Warning Sound System. Retrieved September 28, 2020, from Analog.com website:

<https://www.analog.com/en/analog-dialogue/articles/electric-vehicle-warning-sound-system.html#>

Politecnico, D., Torino, Candidate, A., Massimo, V., & Gnaniah. (2019). *Functional Safety Assessment for Advanced Driver Assistance System*. Retrieved from <https://webthesis.biblio.polito.it/11062/1/tesi.pdf>

Rizul Sharma, & Pratyush Agarwal. (2019, July 3). "DRIVER DROWSINESS DETECTION SYSTEM." Retrieved September 28, 2020, from ResearchGate website:

https://www.researchgate.net/publication/336878674_DRIVER_DROWSINESS_DETECTION_SYSTEM

S. Khastgir, S. Birrell, G. Dhadyalla, & P. Jennings. (2018). The science of testing : an automotive perspective. Retrieved September 28, 2020, from undefined website:

<https://www.semanticscholar.org/paper/The-science-of-testing-%3A-an-automotive-perspective-Khastgir-Birrell/65e769768f9dc183c89b75ec0479ebd4423b9a5f>

SAE. (2018). SAE International Releases Updated Visual Chart for Its "Levels of Driving Automation" Standard for Self-Driving Vehicles. Retrieved September 24, 2020, from Sae.org website: <https://www.sae.org/news/press-room/2018/12/sae-international-releases-updated-visual-chart-for-its-%E2%80%9Clevels-of-driving-automation%E2%80%9D-standard-for-self-driving-vehicles>

Sankaranarayanan Velupillai, & Levent Guvenc. (2008). Tire Pressure Monitoring [Applications of Control]. Retrieved September 28, 2020, from ResearchGate website:

https://www.researchgate.net/publication/3207920_Tire_Pressure_Monitoring_Applications_of_Control

Shaout, A., Colella, D., & Awad, S. (2011). Advanced driver assistance systems - past, present and future. *2011 Seventh International Computer Engineering Conference (ICENCO'2011)*, 72–82(10.1109/ICENCO.2011.6153935).
<https://doi.org/10.1109/icenco.2011.6153935>

Shimizu, T., & Sako, K. (2000). *Kazuhiro sakiyama parking assist system*. Retrieved from <https://www.denso-ten.com/business/technicaljournal/pdf/15-1.pdf>

Sini, J., & Violante, M. (2020). A simulation-based methodology for aiding advanced driver assistance systems hazard analysis and risk assessment. *Microelectronics Reliability*, 109, 113661. <https://doi.org/10.1016/j.microrel.2020.113661>

Skog, I., & Händel, P. (2009, April). In-Car Positioning and Navigation Technologies—A Survey. Retrieved September 28, 2020, from ResearchGate website:
https://www.researchgate.net/publication/224378740_In-Car_Positioning_and_Navigation_Technologies-A_Survey

Smith, K. (2017, June 13). The Importance of Wireless Communication for ADAS and Autonomous Vehicles. Retrieved September 24, 2020, from Allaboutcircuits.com website: <https://www.allaboutcircuits.com/news/the-importance-of-wireless-communication-for-adas-and-autonomous-vehicles/>

Stiawan, R., Adhi Kusumadjati, Nina Siti Aminah, & Sparisoma Viridi. (2019, April). An Ultrasonic Sensor System for Vehicle Detection Application. Retrieved September 24, 2020, from ResearchGate website:
https://www.researchgate.net/publication/332916346_An_Ultrasonic_Sensor_System_for_Vehicle_Detection_Application

VEONEER. (2019). Driver Monitoring Systems. Retrieved September 28, 2020, from Veoneer website: <https://www.veoneer.com/en/driver-monitoring-systems>

Volvo Cars. (2016). Hill Descent Control (HDC). Retrieved September 28, 2020, from [Volvocars.com website: https://www.volvocars.com/se/support/manuals/xc60/2015w17/forarstod/forarstod/hill-descent-control-hdc](https://www.volvocars.com/se/support/manuals/xc60/2015w17/forarstod/forarstod/hill-descent-control-hdc)

- Warren, M. E. (2019, June). Automotive LIDAR Technology. Retrieved September 24, 2020, from ResearchGate website:
https://www.researchgate.net/publication/334754421_Automotive_LIDAR_Technology
- World Health Organization: WHO. (2020, February 7). Road traffic injuries. Retrieved September 23, 2020, from Who.int website: <https://www.who.int/news-room/factsheets/detail/road-traffic-injuries>
- Zador, P. L., Krawchuk, S. A., & Voas, R. B. (2000, August). Automotive Collision Avoidance System (ACAS) Program. Retrieved September 23, 2020, from Nhtsa.com website:
<https://www.nhtsa.gov/DOT/NHTSA/NRD/Multimedia/PDFs/Crash%20Avoidance/2000/ACAS-FinalReport-2000-08.pdf>
- Zigmund Bluvband, & Pavel Grabov. (2009, March). Failure analysis of FMEA. Retrieved September 28, 2020, from ResearchGate website:
https://www.researchgate.net/publication/224441904_Failure_analysis_of_FMEA
- ZMP. (2013). About In-vehicle camera in ADAS. Retrieved August 24, 2020, from ZMP website:
https://www.zmp.co.jp/en/knowledge/adas_dev/adas_sensor/adas_camera

ANEXOS



AVAL DEL TUTOR PARA LA PRESENTACIÓN DE TESIS

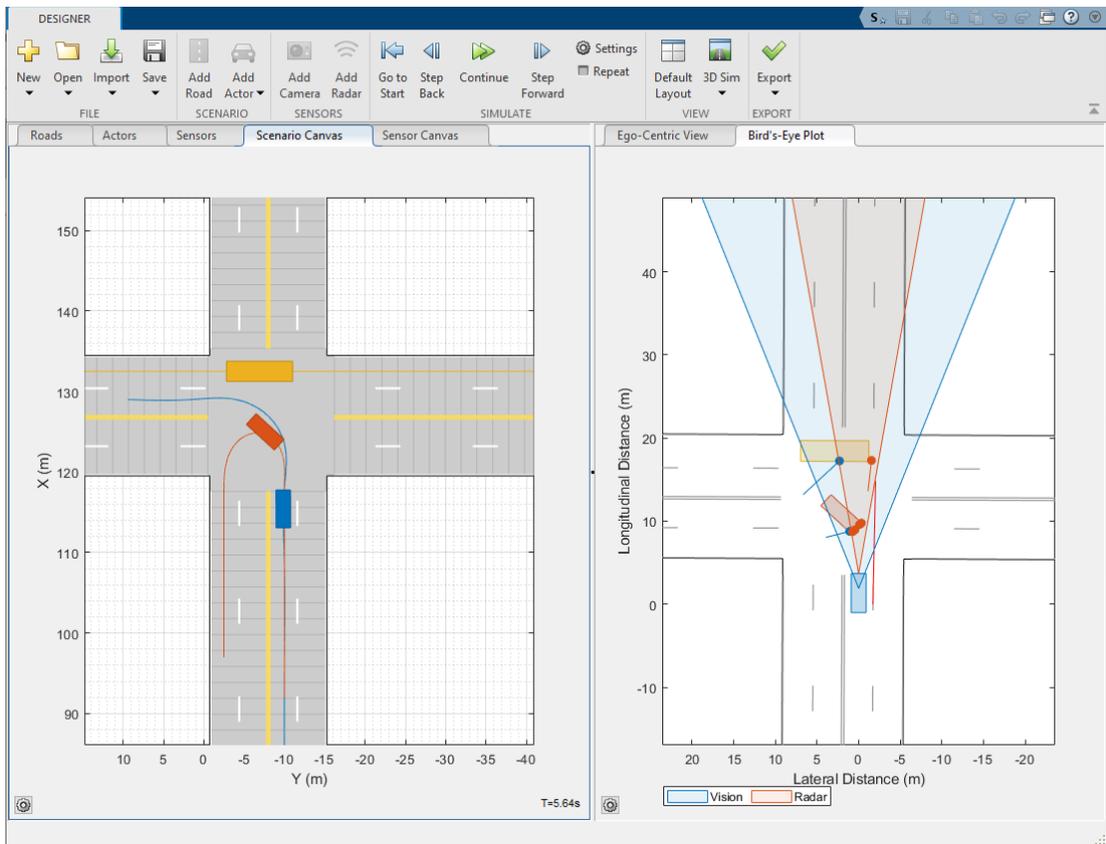
En mi calidad de tutor de la tesis presentada por: Adiac E. Aguilar González, para optar al grado de licenciatura en Ingeniería Industrial doy fe que el informe final de la tesis: “**Análisis de Seguridad y Evaluación de Riesgos para el Sistema Avanzado de Asistencia al Conductor – ADAS**”, posee la calidad científica y metodológica para ser sometido a la revisión y evaluación por los miembros del jurado examinador que se designe.

Dado en la ciudad de Managua ,a los once días del mes de octubre *de dos mil veinte.*

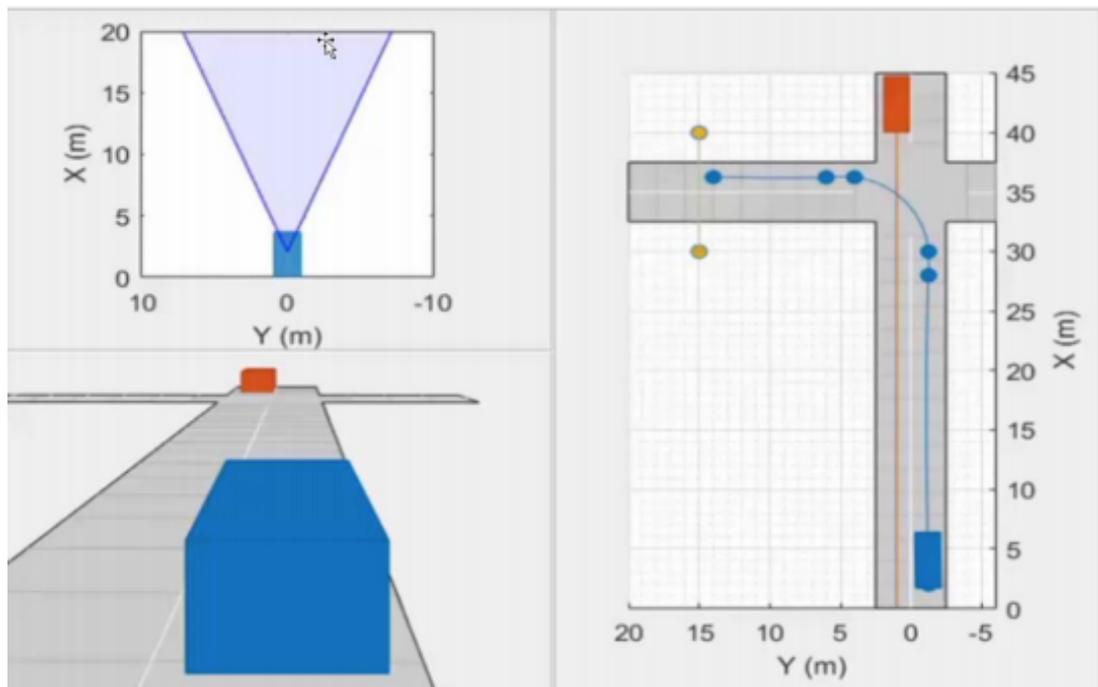
Atentamente

Marlon José Velásquez Reynoza

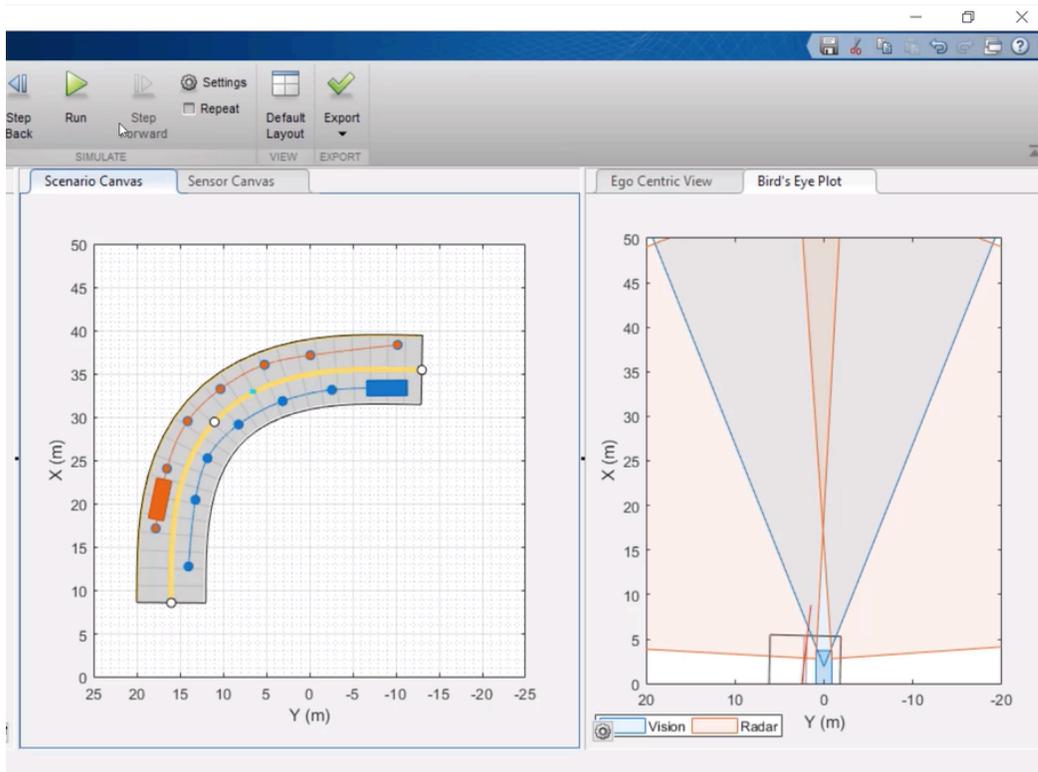
Nombres y apellidos
Marlon Velasquez R.
Firma del director de tesis



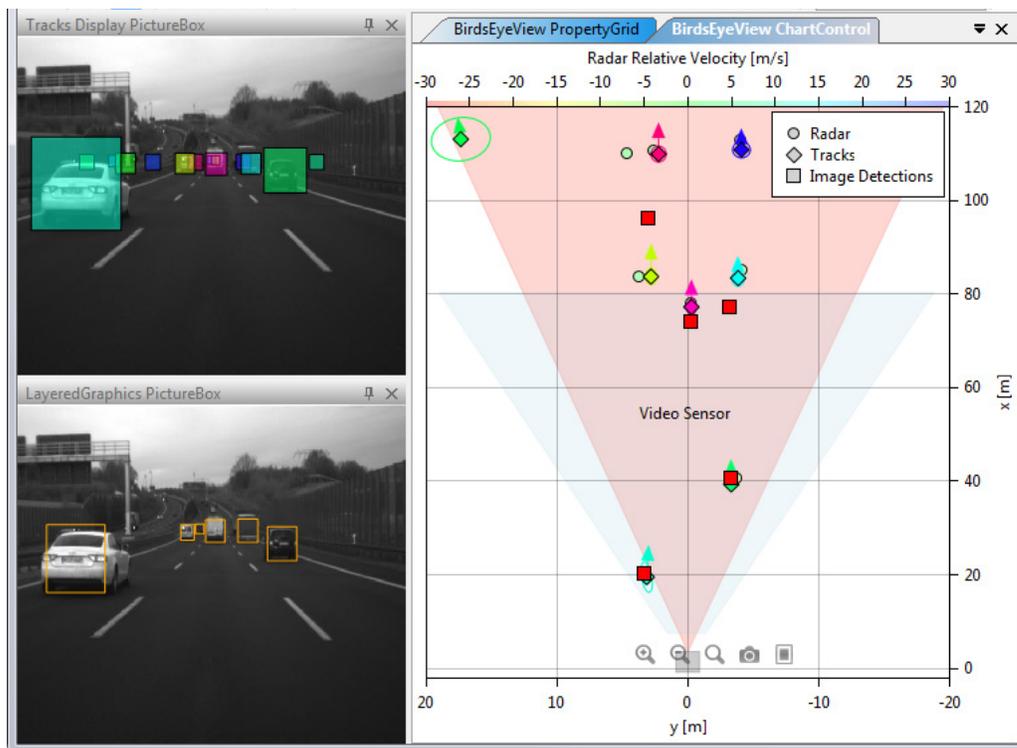
Anexo 1 Simulación de 4 vías en plataforma Simulink



Anexo 2 Simulación de giro en intersección en plataforma Simulink



Anexo 4 Simulación de curva en plataforma Simulink



Anexo 5 Simulación de identificación y clasificación de objetos múltiples en plataforma Simulink



Anexo 7 Simulación de 4 vías en plataforma CARLA



Anexo 8 Simulación de giro 90° en plataforma CARLA



Anexo 9 Simulación de giro zigzag en plataforma CARLA



Anexo 10 Simulación de curva en plataforma CARLA

Nota: Para cada pregunta se considera la escala de 1 a 5, donde:

1. Muy Poco	2. Poco	3.Regular	4.Aceptable	5.Excelente
-------------	---------	-----------	-------------	-------------

Dpto. FuSa						
No	ITEM TESIS	Puntaje				
		1	2	3	4	5
1	Identificación y clasificación efectiva de las causas de falla					X
2	Resultado de análisis de modos de falla y valores individuales G – F – D					X
3	Valor promedio NPR, resultante de análisis grupal en colaboración con departamentos multi funcionales de Zenuity				X	
4	Acción Correctora propuesta a causa de modos de fallas en análisis FMEA					X
5	Identificación y clasificación de Escenarios Peligrosos HAZOP, pre estudio - HARA					X
6	Análisis y valoración de S, E & C para cada uno de los escenarios peligrosos identificados					X
7	Documentación de análisis de fallas asociados a items					X
8	Elaboración de propuestas de objetivos de seguridad					X

Apellido y Nombre	Hákan Sivencrona +46 0760065001	Oficial de Seguridad FuSa	
Departamento	En representación del Dpto. FuSa	Zenuity	

Anexo 11

Dpto. Software Development						
No	ITEM TESIS	Puntaje				
		1	2	3	4	5
1	Identificación y clasificación efectiva de las causas de falla				X	
2	Resultado de análisis de modos de falla y valores individuales G – F – D					X
3	Valor promedio NPR, resultante de análisis grupal en colaboración con departamentos multi funcionales de Zenuity					X
4	Acción Correctora propuesta a causa de modos de fallas en análisis FMEA				X	
5	Identificación y clasificación de Escenarios Peligrosos HAZOP, pre estudio - HARA					X
6	Análisis y valoración de S, E & C para cada uno de los escenarios peligrosos identificados					X
7	Documentación de análisis de fallas asociados a items					X
8	Elaboración de propuestas de objetivos de seguridad					X

Apellido y Nombre	Erik Coelingh +46 0709677432	Gerente de Software Development	
Departamento	En representación del Dpto. Software Development	Zenuity	

Anexo 12

Dpto. UX & UI						
No	ITEM TESIS	Puntaje				
		1	2	3	4	5
1	Identificación y clasificación efectiva de las causas de falla			X		
2	Resultado de análisis de modos de falla y valores individuales G – F – D				X	
3	Valor promedio NPR, resultante de análisis grupal en colaboración con departamentos multi funcionales de Zenuity				X	
4	Acción Correctora propuesta a causa de modos de fallas en análisis FMEA					X
5	Identificación y clasificación de Escenarios Peligrosos HAZOP, pre estudio - HARA					X
6	Análisis y valoración de S, E & C para cada uno de los escenarios peligrosos identificados				X	
7	Documentación de análisis de fallas asociados a ítems				X	
8	Elaboración de propuestas de objetivos de seguridad					X

Apellido y Nombre	Marcus Nilsson +46 0760674007	Líder de UX & UI	
Departamento	En representación del Dpto. UX & UI	Zenuity	

Anexo 13

Dpto. R&D						
No	ITEM TESIS	Puntaje				
		1	2	3	4	5
1	Identificación y clasificación efectiva de las causas de falla					X
2	Resultado de análisis de modos de falla y valores individuales G – F – D			X		
3	Valor promedio NPR, resultante de análisis grupal en colaboración con departamentos multi funcionales de Zenuity				X	
4	Acción Correctora propuesta a causa de modos de fallas en análisis FMEA				X	
5	Identificación y clasificación de Escenarios Peligrosos HAZOP, pre estudio - HARA					X
6	Análisis y valoración de S, E & C para cada uno de los escenarios peligrosos identificados					X
7	Documentación de análisis de fallas asociados a items					X
8	Elaboración de propuestas de objetivos de seguridad				X	

Apellido y Nombre	Mats Nordlund +46 0768641773	Jefe de Ingenieros de R&D +46 0792345138	
Departamento	En representación del Dpto. R&D	Zenuity	

Anexo 14

HÅKAN SIVENCRONA
ZENUITY

Lindholmospiren 2, 417 56 Göteborg
zenseact.com.

TO OUR DEAREST STUDENTS,

It has been amazing to collaborate with such amazing minds

I enthusiastically offer this letter in support of Adiac Aguilar who did a research thesis about, "A Safety & Risk Assessment for ADAS systems" in collaboration with Zenuity. Adiac developed his research under the FuSa department of Zenuity and under my watch. At Zenuity, we found him as a creative and industrious student who showed a natural flair for both safety and innovation in the automotive industry.

His research had contributed in the continuous development and optimization of the ADAS - AD systems. By identifying different scenarios and hazardous conditions in the concept phase, it provides a systematic approach to this unusual scenarios and it expands the understanding of the system to overcome this hazards.

A brilliant, highly motivated student whose curiosity for innovation and technology contributes in the journey of the developing of a safe self driving vehicle. As part of the FuSa department, we wanted to thanks Adiac for his contributions and we wish him the best of luck for his upcoming projects.

BEST,

Håkan Sivencrona
Safety Engineer - Zenuity



Filename: Adiac Aguilar G - TESIS ADAS SAFETY UAM.doc
Directory: /Users/adiacaguilar/Library/Containers/com.microsoft.Word/Data/
Documents
Template: /Users/adiacaguilar/Library/Group
Containers/UBF8T346G9.Office/User
Content.localized/Templates.localized/Normal.dotm
Title:
Subject:
Author: Adriana Rizo
Keywords:
Comments:
Creation Date: 11/2/20 3:34:00 PM
Change Number: 2
Last Saved On: 11/2/20 3:34:00 PM
Last Saved By: Microsoft Office User
Total Editing Time: 1 Minute
Last Printed On: 11/2/20 3:34:00 PM
As of Last Complete Printing
Number of Pages: 171
Number of Words: 27,486 (approx.)
Number of Characters: 156,674 (approx.)