FUNCTIONAL SAFETY FOR AUTONOMOUS DRIVING

Dr. Justyna Zander, NVIDIA | January 30, 2017

IS&T Int. Symposium on Electronic Imaging 2017; Autonomous Vehicles and Machines 2017; 29 January - 2 February, 2017 • Burlingame, CA, USA
FULL AUTONOMY WITH FUNCTIONAL SAFETY

Automated Driving Assistance Systems ERA

- Machine monitors human
  - Great

Prototypical Autonomy ERA

- Self-driving prototypes
  - Very limited in use

Safe and Certified Autonomous Driving ERA

- AI-based machine in control
  - Amazing!
Functional Safety is the absence of unreasonable risk due to hazards caused by malfunctioning behavior of electrical and electronic systems.

The objective of functional safety is freedom from unacceptable risk of physical injury or of damage to the health of people either directly or indirectly (through damage to property or to the environment).

Functional safety is intrinsically end-to-end in scope in that it has to treat the function of a component or subsystem as part of the function of the whole system.

FUNCTIONAL SAFETY HIGHLIGHTS

Development Process

- Traceable processes and certifiable coding are complex

Classified Tools

- Tools require ISO26262 qualification

Functional Safety Design

- Safety design must be included in the system-level design

AUTONOMOUS DRIVING PIPELINE

SENSE

LOCALIZE

PERCEIVE

MAP

PLAN

CONTROL
END-TO-END DEEP LEARNING PLATFORM FOR SELF-DRIVING CARS

NVIDIA® DGX-1™
NVIDIA® DIGITS

NVIDIA® DRIVE™ PX 2 | NVIDIA® Xavier

NVIDIA® DRIVEWORKS
- Perception
- Localization
- Planning
- Visualization

NVIDIA® DriveWorks
COMBO: 3D VEHICLE, LANES, OPEN ROAD
NVIDIA® DRIVE™ PX 2

12 CPU cores | Pascal GPU | 8 TFLOPS | 24 DL TOPS | 16nm FF | 250W

World’s First AI Supercomputer for Self-Driving Cars
NVIDIA DRIVEWORKS SOFTWARE STACK

DriveWorks Tools

Other Sensors → DriveWorks Dataflow Layer

Cameras → DriveWorks Dataflow Layer

DriveWorks Modules, NVDRIVENET

Computer Vision Primitives

OpenGL ES, CUDA

cuDNN

HW
V4L SDK
DriveWorks
Applications
UNINTENDED ACCELERATION

Case Study

Sudden unintended acceleration is the unintended, unexpected, uncontrolled acceleration of a vehicle, often accompanied by an apparent loss of braking effectiveness.

It may be caused by mechanical, electrical, or electronic problems, driver error (e.g., pedal misapplication), or some combination of these factors.
UNINTENDED ACCELERATION
Case Study
UNINTENDED ACCELERATION

Case Study

Hazard: Unintended acceleration and loss of braking effectiveness.

Safety goal: Mitigate the risk of an unintended acceleration.

Safety requirements: ???
Unintended Acceleration

OR

Braking system failure

OR

Throttle system failure

OR

Brake pedal failure

OR

Brake switch failure

OR

Throttle pedal failure

OR

Incorrect throttle angle calculation
Hazard: Unintended acceleration and loss of braking effectiveness.

Safety goal: Mitigate the risk of an unintended acceleration.

Safety requirements:

Vehicle longitudinal acceleration shall not exceed driver demand by 1.3 m/s² for longer than 1s (ASIL B).
SAFETY DESIGN PATTERN

[Diagram showing process flow with blocks for Signal Plausibility Check, Detect Failure, Fallback Strategy, React: Mitigate | Heal, and ASIL assignment. Arrows indicate the flow: longitudinal acceleration and throttle angle.]
**UNINTENDED ACCELERATION**

Case Study

**Hazard:** Unintended acceleration and loss of braking effectiveness.

**Safety goal:** Mitigate the risk of an unintended acceleration.

**Safety requirements:**

Vehicle longitudinal acceleration shall not exceed driver demand by 1.3 m/s² for longer than 1s (ASIL B).

Within time budget of 1.001s detect the scenario where the vehicle positive longitudinal acceleration exceeds driver demand by 1.3 m/s² for longer than 1s.

Within time budget of 0.1s mitigate to safe state, where safe state is: shut off the acceleration by shutting down the throttle (ASIL B).
SAFETY DESIGN EXAMPLE FOR UNINTENDED ACCELERATION

- Determine the acceleration request
  - Sensor A
- Calculate the acceleration value
- Determine the throttle angle
  - Control chip
- Position the output throttle angle
  - ADC1
- Shut down throttle
  - Safety chip
- Compare the acceleration calculation results
- Determine the throttle angle using additional signal source
  - Sensor B
- Hardware
- Safety Design
- Functionality
WHAT IS NEXT?
8 Core Custom ARM64 CPU
512 Core Volta GPU
Designed for ASIL D Functional Safety
30 TOPS DL | 30W
SOFTWARE STACK - 30,000’ ROADMAP

Common foundation | OS agnostic VM services | OEM Guest OSs
European New Car Assessment Program (EURO NCAP) 2018
WHAT ELSE IS NEXT?

“YOUR TIME IS COMING. DO NOT BE LATE!” ☺️
AUTONOMOUS DRIVING ECOSYSTEM

- IHVs
- OEMs
- ISVs
- Researchers
- SW Companies
- Tier 1s

Technology Provider (NVIDIA)
Thank you!

justynaz@nvidia.com
NVIDIA DRIVEWORKS SOFTWARE STACK

NVIDIA DRIVEWORKS SDK

PERCEPTION
Sensor Fusion
Objects (NVDRIVENet)
Segmentation

LOCALIZATION
Map Fusion
Landmarks (NVDRIVENet)
GPS Trilateration

PLANNING
Trajectory
Behavior (NVDRIVENet)
Mission

VISUALIZATION

NVIDIA System Software

Autonomous Driving Applications
AUTONOMOUS DRIVING ECOSYSTEM

DEVELOPERS

Researchers
ISVs
IHVs
Drive PX
DriveWorks SDK

CUSTOMERS

OEMs
SW Companies
Tier 1s
Drive PX

Value Creation

Demand Gen