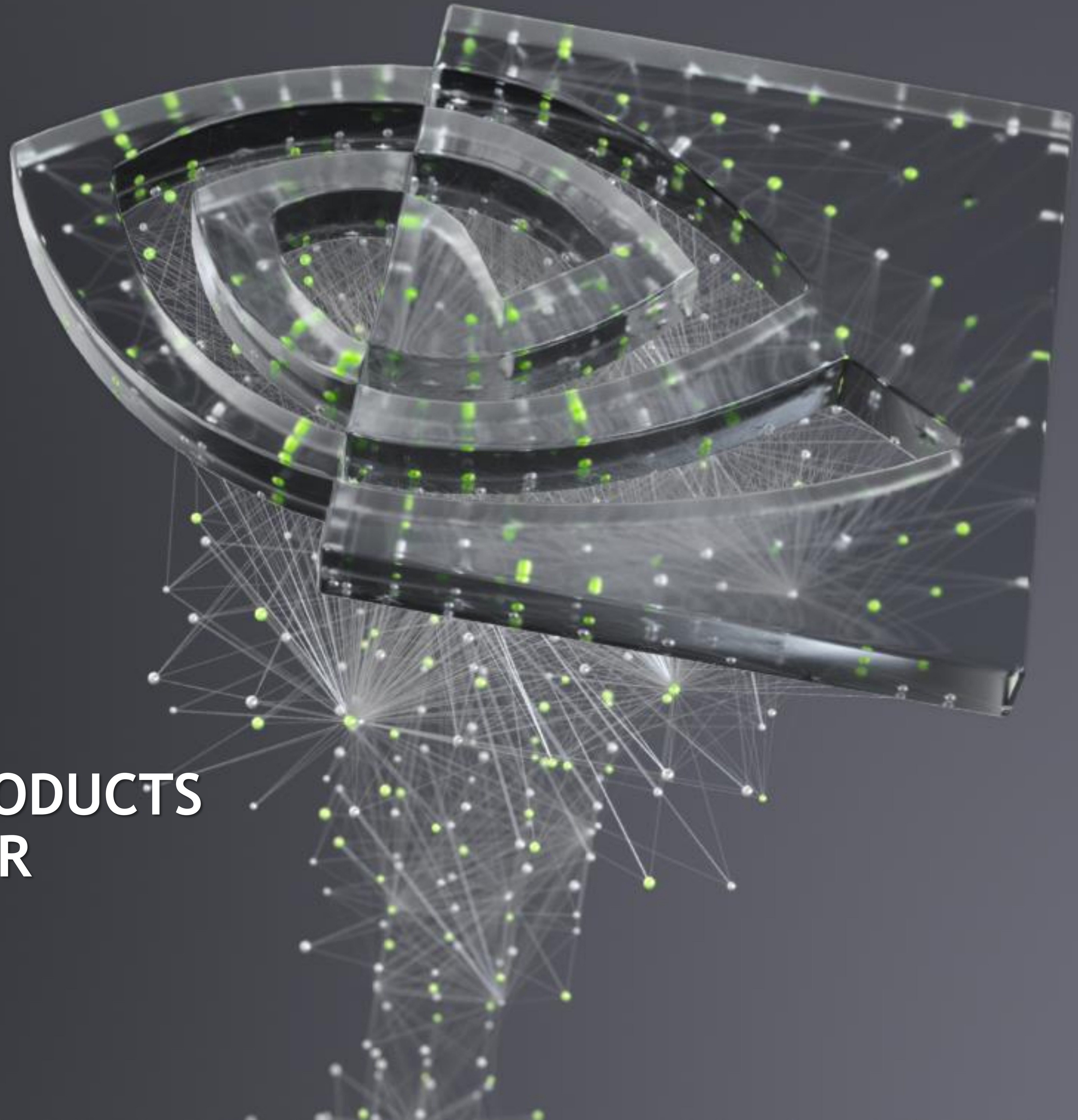


NVIDIA DRIVE SAFETY 360: HOW NVIDIA CREATES THE PRODUCTS THAT MAKE YOUR DRIVE SAFER

Karl Greb, Safety Engineering Director

21st September 2020

AGENDA

Introduction to NVIDIA’s Safety Efforts

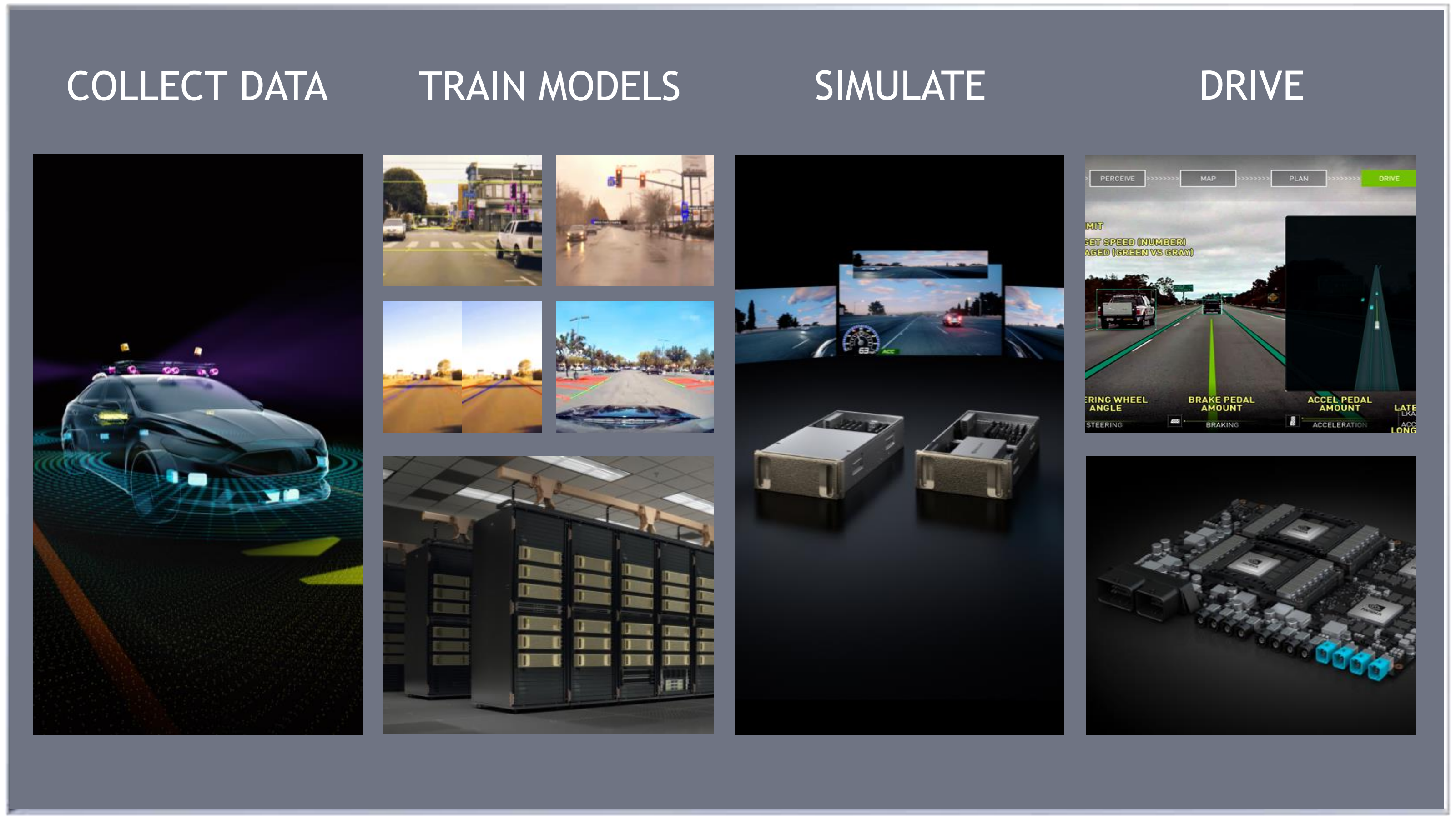
Process (Systematic) Compliance

Concept (Architecture) and Product Compliance

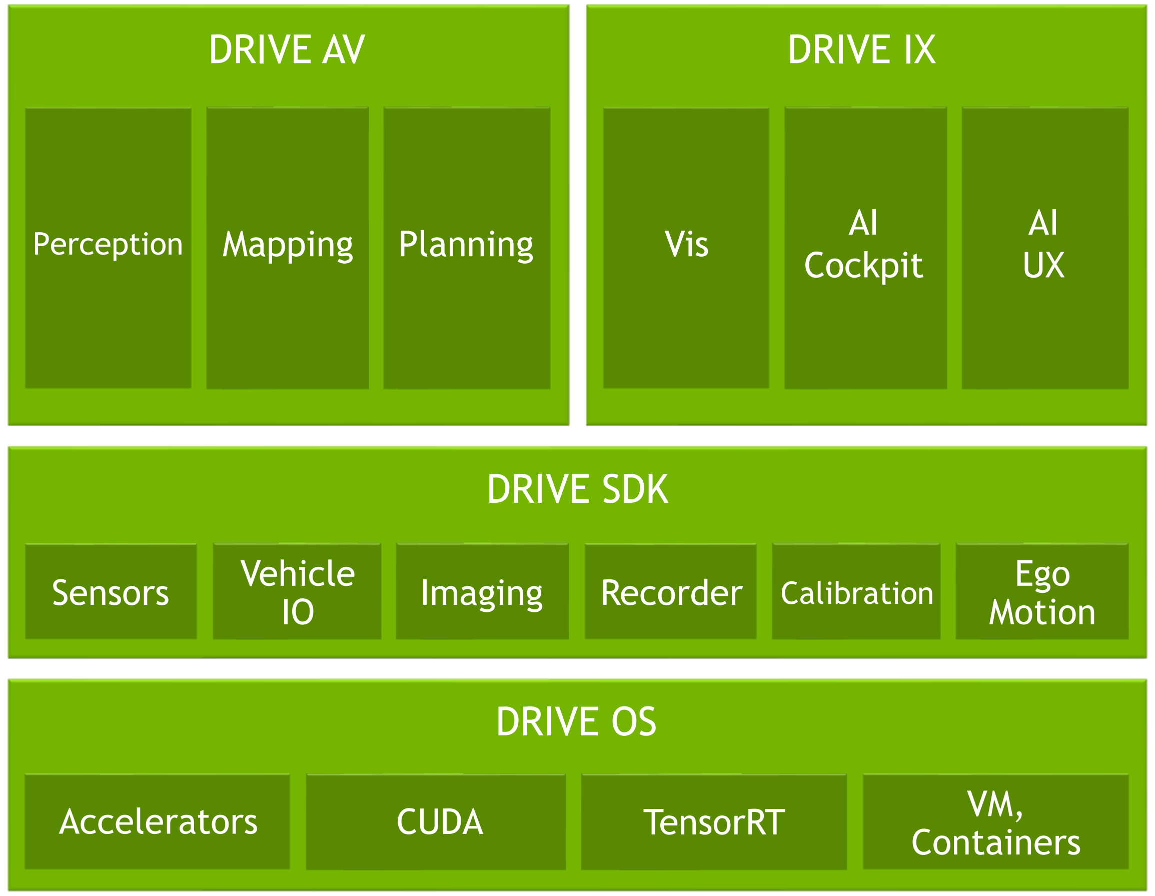
Deeper Dive: Making a Compliant SoC

Summary

NVIDIA DRIVE
SOFTWARE-DEFINED AV PLATFORM



End-to-End Infrastructure



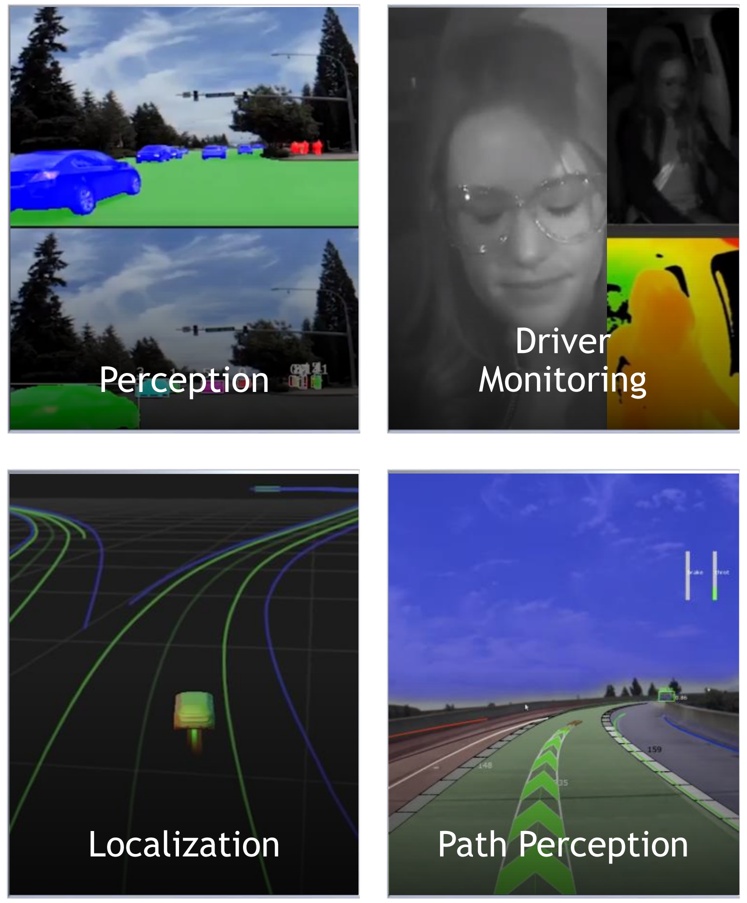
DRIVE AV
Perception
Mapping
Planning

DRIVE IX
Vis
AI Cockpit
AI UX

DRIVE SDK
Sensors
Vehicle IO
Imaging
Recorder
Calibration
Ego Motion

DRIVE OS
Accelerators
CUDA
TensorRT
VM, Containers

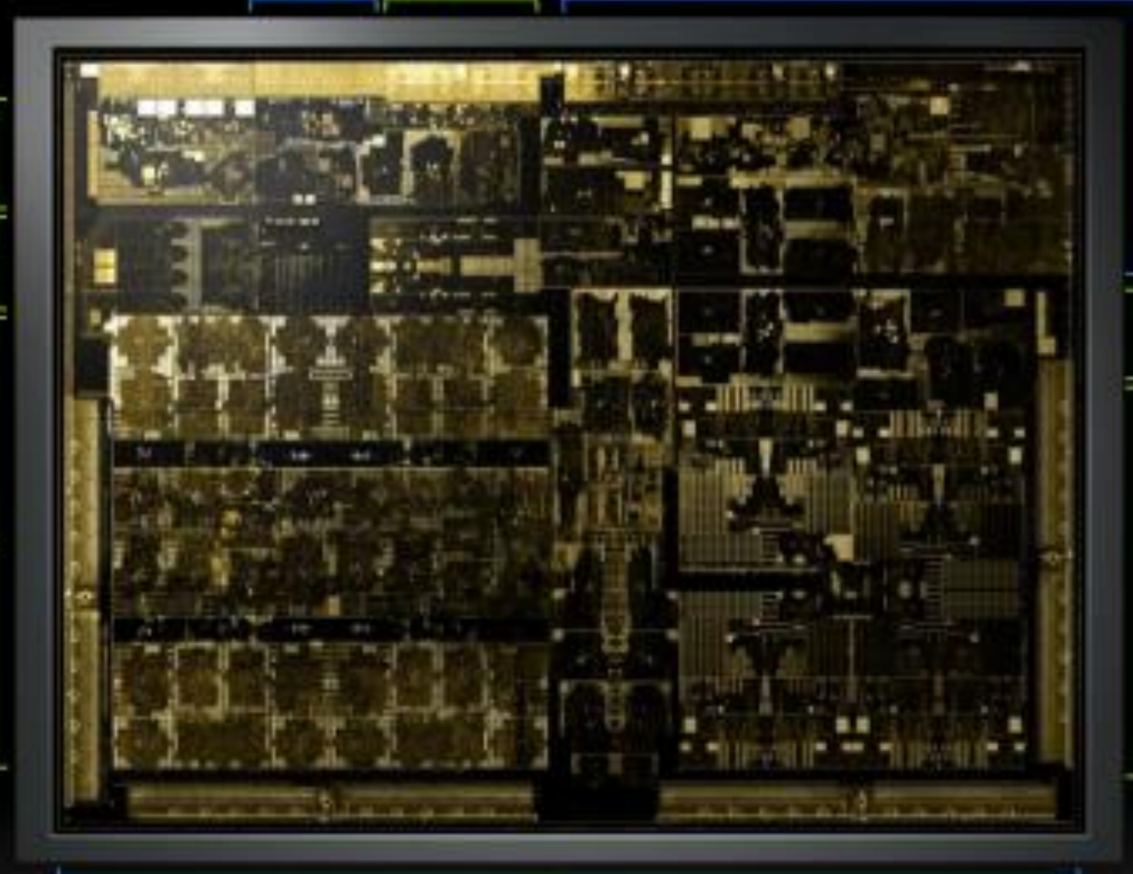
Open Software Program



Pre-Trained Models

XAVIER

World's First Autonomous Machines Processor



16 Lane CSI
109 Gbps CPHY 1.1
1Gb Ethernet

DLA
5.7 TFLOPS FP16
11.4 TOPS INT8

Multimedia Engines
1.2 GPIX/s Encode
1.8 GPIX/s Decode
4 GPIX/s Video Image Compositor

Vision Accelerator
1.7 TOPS

Stereo & Optical Flow Engine
2x 3.1 TOPS

Volta Tensor Core GPU
FP32 / FP16 / INT8 Multi-Precision
512 CUDA Tensor Cores
2.8 CUDA TFLOPS (FP16)
22.6 Tensor Core DL TOPS

Industry Standard High-Speed IO
PCIe Gen4 Root and Endpoint
USB 3.1 gen2 Host and Device
UFS 2.1 Embedded Storage

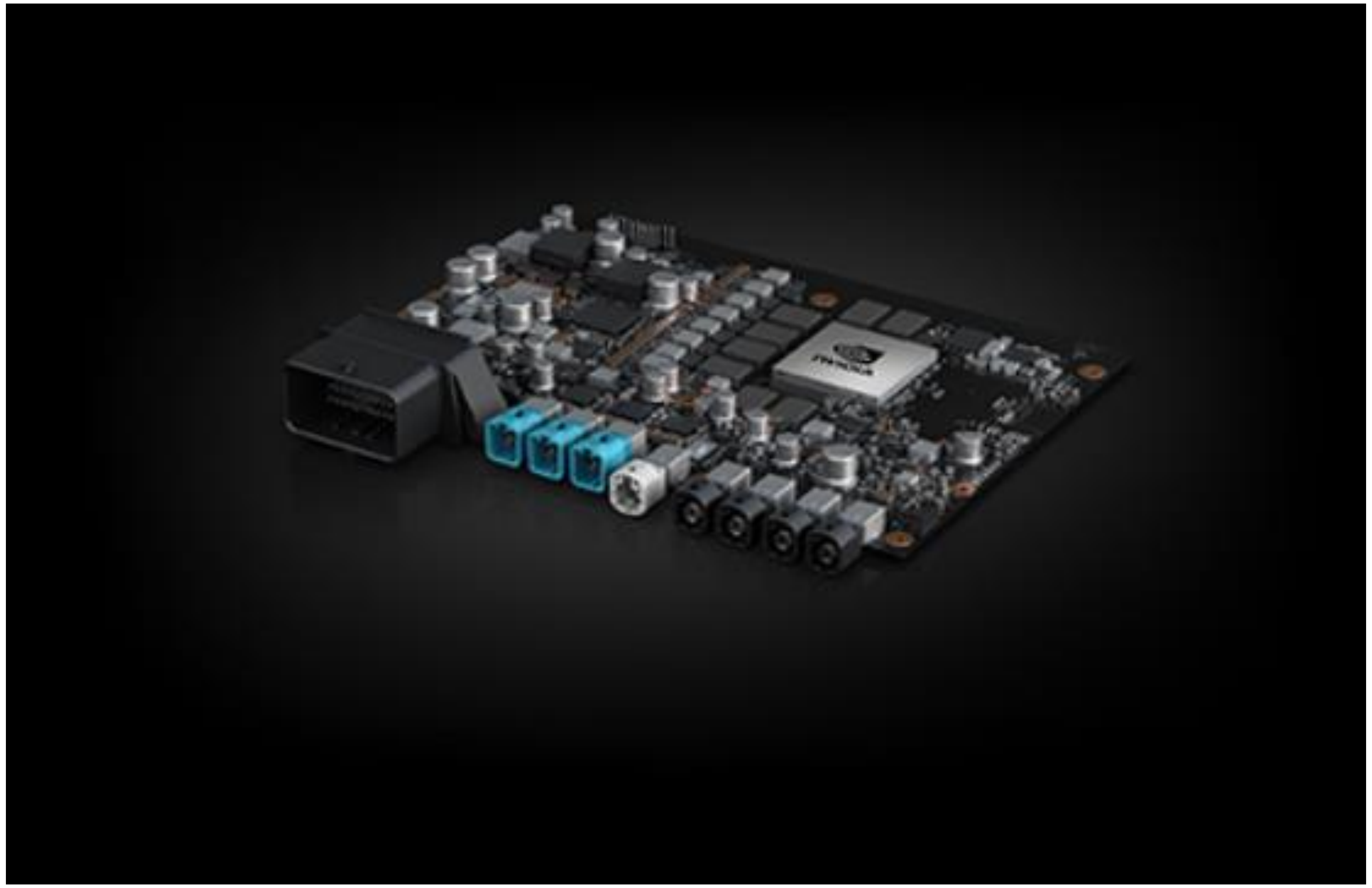
ISP
2.4 GPIX/s
Native Full-range HDR
Tile-based Processing

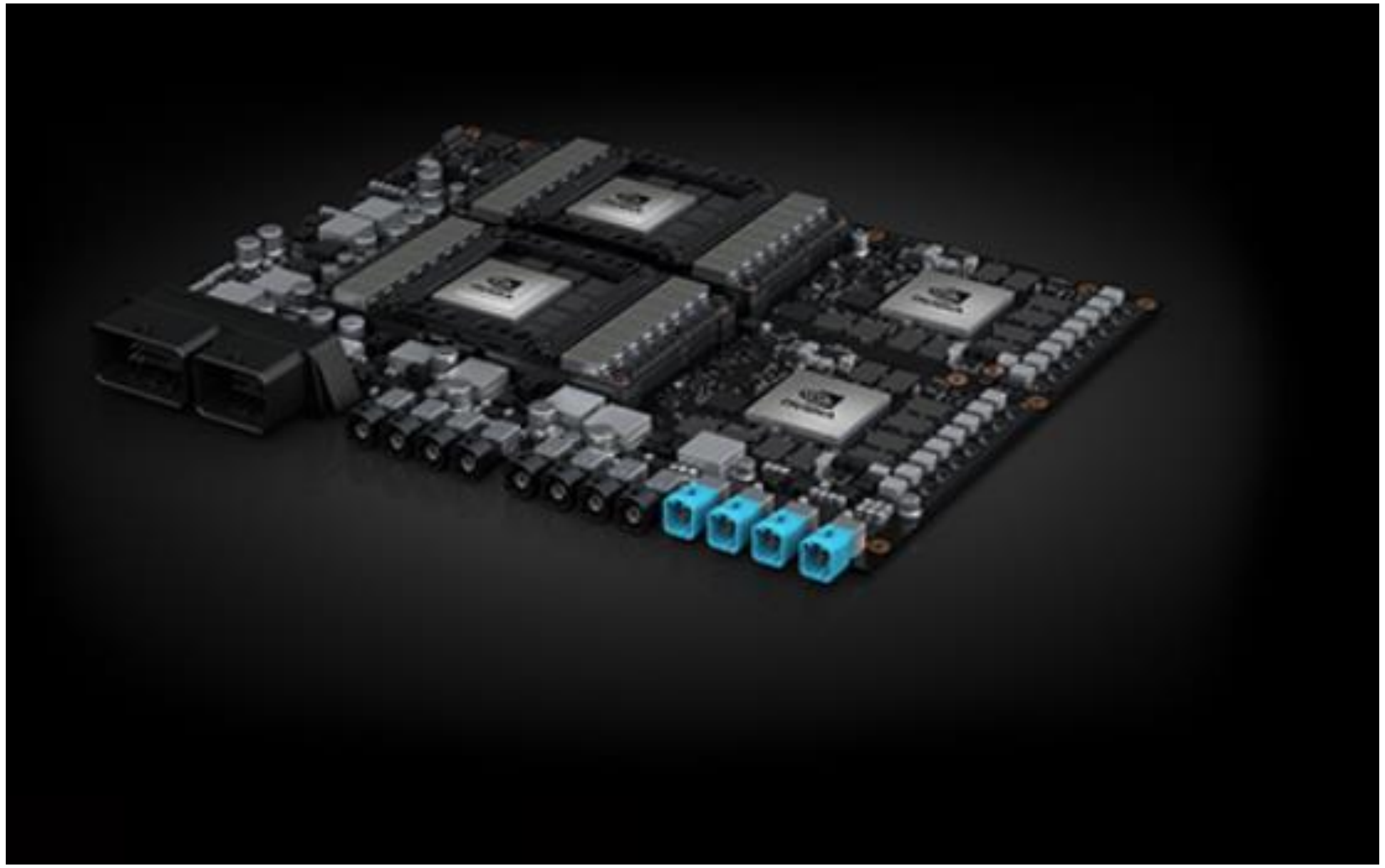
Carmel ARM64 CPU
8 Cores
10-wide Superscalar
21 SpecInt2K6 (est.)

256-Bit LPDDR4X
137 GB/s

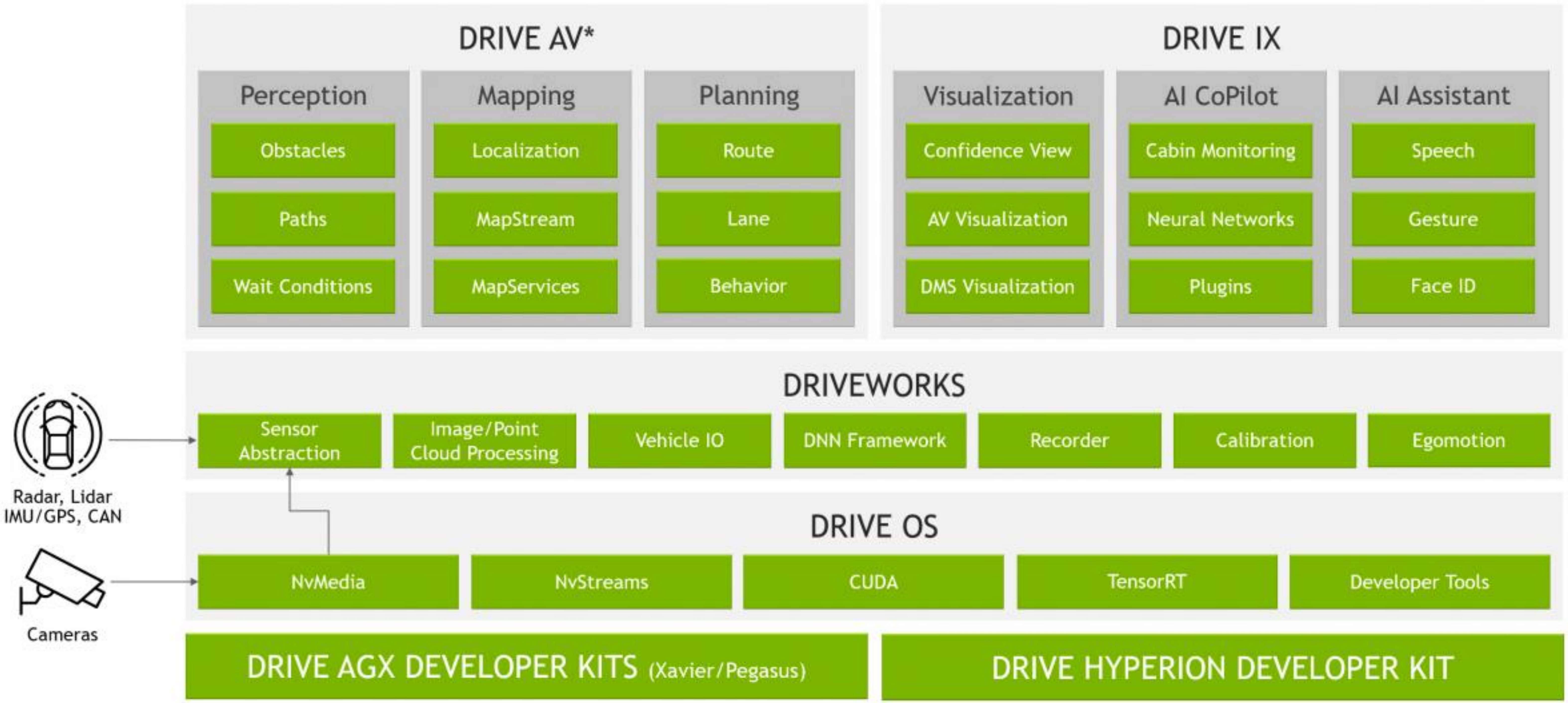
Most Complex SOC Ever Made | 9 Billion Transistors, 350mm^2, 12FFN | ~8,000 Engineering Years

DRIVE AGX XAVIER AND DRIVE AGX PEGASUS





DRIVE OS



DRIVE AV*

Perception

Obstacles

Paths

Wait Conditions

Mapping

Localization

MapStream

MapServices

Planning

Route

Lane

Behavior

DRIVE IX

Visualization

Confidence View

AV Visualization

DMS Visualization

AI CoPilot

Cabin Monitoring

Neural Networks

Plugins

AI Assistant

Speech

Gesture

Face ID

DRIVEWORKS

Sensor Abstraction

Image/Point Cloud Processing

Vehicle IO

DNN Framework

Recorder

Calibration

Egomotion

DRIVE OS

NvMedia

NvStreams

CUDA

TensorRT

Developer Tools

DRIVE AGX DEVELOPER KITS (Xavier/Pegasus)

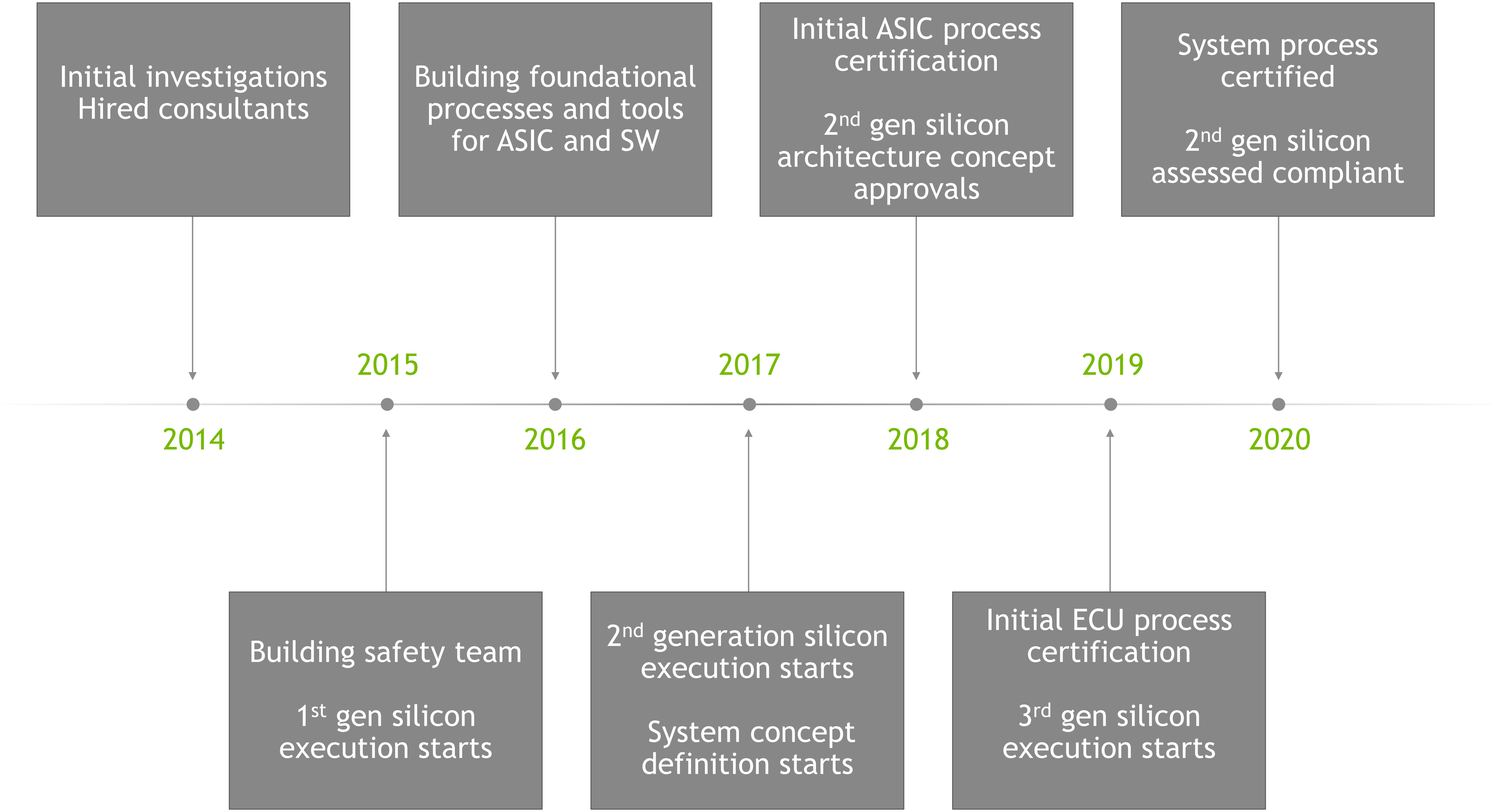
DRIVE HYPERION DEVELOPER KIT

Radar, Lidar
IMU/GPS, CAN

Cameras

DRIVE AV modules are an extension of the DriveWorks SDK in DRIVE Software releases

LONG TERM INVESTMENT



2014

Initial investigations
Hired consultants

2015

Building safety team

1st gen silicon execution starts

2016

Building foundational processes and tools for ASIC and SW

2017

2nd generation silicon execution starts

System concept definition starts

2018

Initial ASIC process certification

2nd gen silicon architecture concept approvals

2019

Initial ECU process certification

3rd gen silicon execution starts

2020

System process certified

2nd gen silicon assessed compliant

ESTABLISHING TRUST VIA ASSESSMENT

- Arguments for safety compliance for autonomous driving are complex and hard to understand
- Open, independent assessment is critical to earning trust from integrators and the public
- ISO 26262 requires independent assessment of compliance
  - Internal – performed by independent auditors inside company
  - External – performed by trusted safety experts from an accredited assessment body
- NVIDIA prefers external assessment whenever possible – both for our own products and for our suppliers

KEEPING UP WITH STATE OF THE ART

Investment in Standards

- Industry standards groups provide a forum for technical discussion on improving approaches for safety development
- NVIDIA contributes heavily to:
  - ISO 26262 – Road Vehicles, Functional Safety (US, IT, and DE national groups)
  - ISO 21448 – Safety of the Intended Functionality (US, IT, and DE national groups)
  - ISO/TR 4804 – Safety and Cybersecurity for Automated Driving Systems (US and IT groups)
  - IEC 61508 – Functional Safety of E/E/PE Safety-Related Systems (US and IT groups)
  - IEEE P2846 – Assumptions for Models in Safety-Related Automated Vehicle Behavior
  - IEEE P2851 – Exchange/Interoperability Format for Safety Analysis and Safety Verification of IP, SoC, and Mixed Signal Ics

FROM AUTOMOTIVE TO OTHER MARKETS

Leveraging Our Safety Investments

- Automotive is not NVIDIA's only safety critical market.
- Industrial machinery and robotics markets rely on standards which have similar requirements to automotive.
- With minor tailoring, the safety cases for NVIDIA's HW and SW products can be used to make machinery and robotics safer.

<table>
<tr><th>Automotive</th><th colspan="2">Industrial/robotics</th></tr>
<tr><th>ISO 26262</th><th>IEC 61508</th><th>ISO 13849</th></tr>
<tr><td>QM</td><td>-</td><td>-</td></tr>
<tr><td>ASIL A</td><td>SIL 1</td><td>PL B, C</td></tr>
<tr><td rowspan="2">ASIL B</td><td rowspan="3">SIL 2</td><td rowspan="3">PL D</td></tr>
<tr></tr>
<tr><td rowspan="2">ASIL C</td></tr>
<tr><td rowspan="3">SIL 3</td><td rowspan="3">PL E</td></tr>
<tr><td rowspan="2">ASIL D</td></tr>
<tr></tr>
<tr><td>-</td><td>SIL 4</td><td>-</td></tr>
</table>

WHY PROCESS (SYSTEMATIC) COMPLIANCE?

- Systematic faults are the root of majority of real-world incidents resulting in recall or injury
- Robust processes with multiple layers of checks and balances are our best defense against systematic faults
- Regular audits and assessments help to ensure we are effectively applying our processes for systematic fault mitigation.

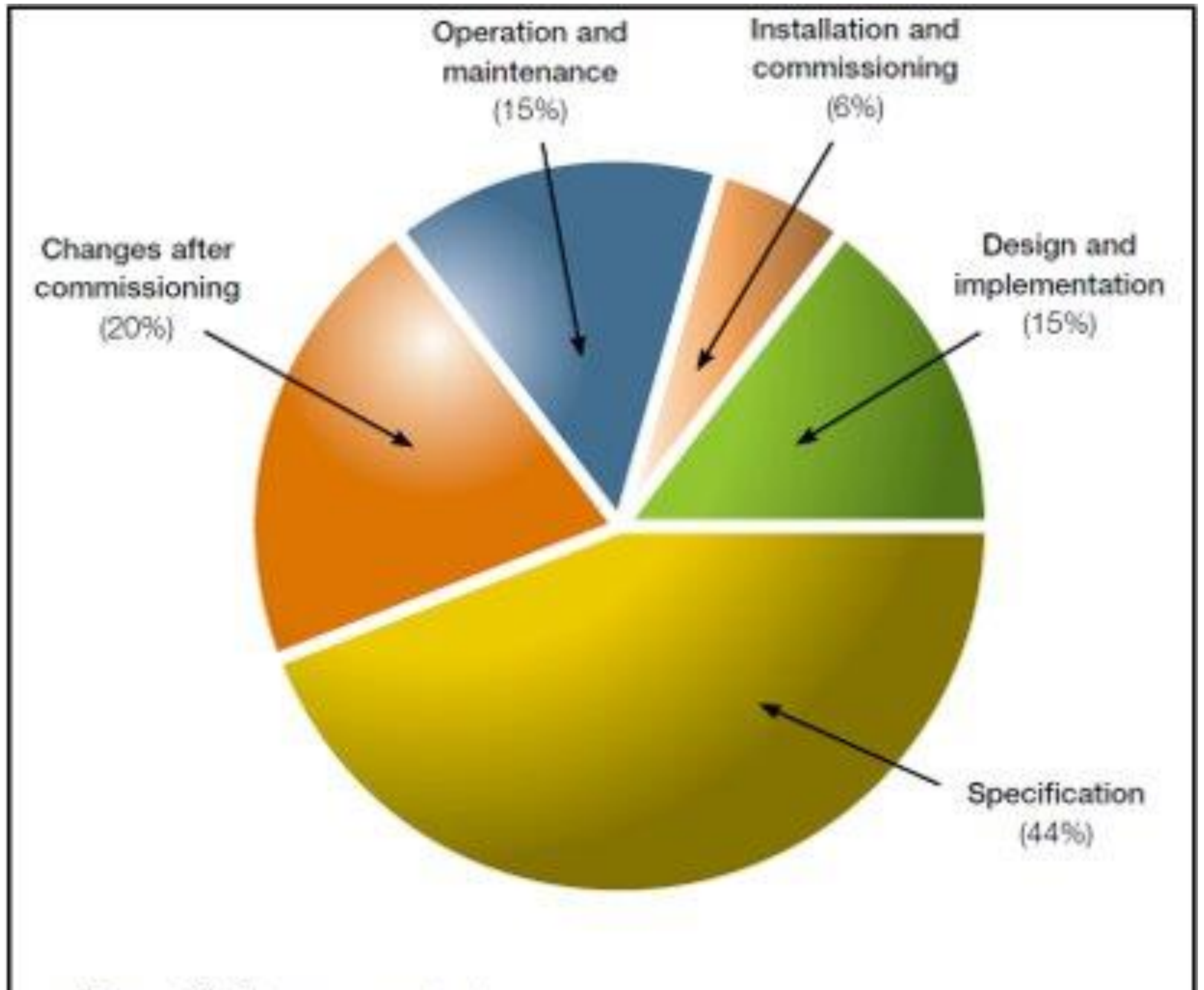


Figure 10 Primary cause by phase

"Out of Control – Why control systems go wrong and how to prevent failure", UK HSE, second edition, 2003

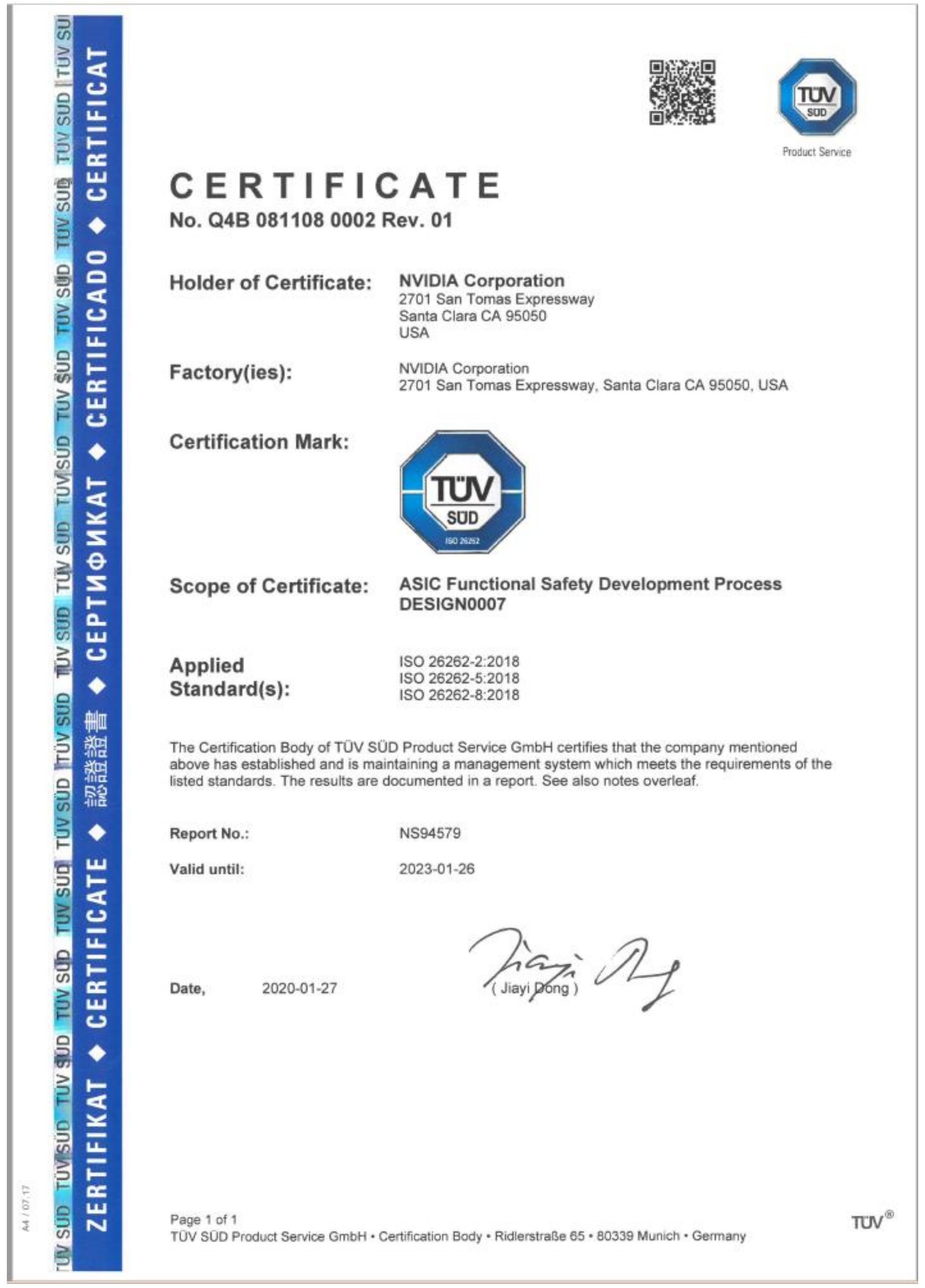
HOW TO DEMONSTRATE PROCESS COMPLIANCE?

- NVIDIA engages industry expert safety assessors to provide independent confirmation

- These external experts evaluate compliance through:
    - Technical evaluation of process documents, work product templates, and training materials
    - On-site audits to confirm effective process implementation
    - Annual inspections check for continued application of process and continuous improvement

ASIC PROCESS COMPLIANCE

- Our DESIGN0007 process provides guidance how to develop ISO 26262 compliant SoCs and dGPUs
- Applied to Xavier SoC and Turing dGPU, as well as upcoming products.
- Originally certified in October 2018 for up to ASIL D capability
- Re-certified in 2019 for ISO 26262 2nd ed. (published December 2018)



ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

TÜV SÜD Product Service

CERTIFICATE
No. Q4B 081108 0002 Rev. 01

Holder of Certificate: NVIDIA Corporation
2701 San Tomas Expressway
Santa Clara CA 95050
USA

Factory(ies): NVIDIA Corporation
2701 San Tomas Expressway, Santa Clara CA 95050, USA

Certification Mark: TÜV SÜD ISO 26262

Scope of Certificate: ASIC Functional Safety Development Process
DESIGN0007

Applied Standard(s): ISO 26262-2:2018
ISO 26262-5:2018
ISO 26262-8:2018

The Certification Body of TÜV SÜD Product Service GmbH certifies that the company mentioned above has established and is maintaining a management system which meets the requirements of the listed standards. The results are documented in a report. See also notes overleaf.

Report No.: NS94579

Valid until: 2023-01-26

Date, 2020-01-27

(Jiayi Dong)

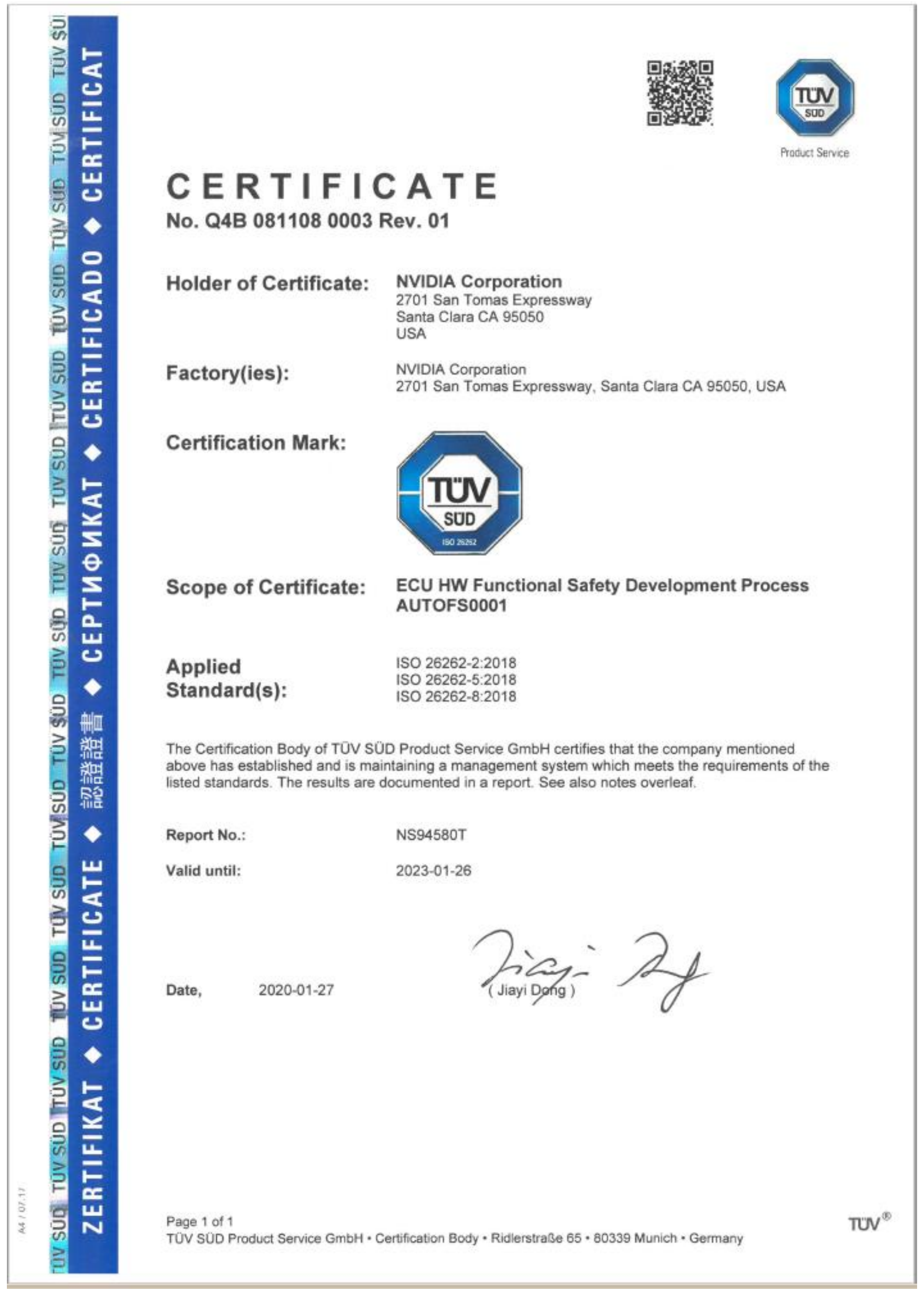
Page 1 of 1
TÜV SÜD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany

A4 / 07.17

TÜV®

ECU PROCESS COMPLIANCE

- Our AUTOFS0001 process provides guidance how to develop ISO 26262 compliant ECUs/boards/modules
- Applied to DRIVE AGX Xavier and DRIVE AGX Pegasus, as well as upcoming products
- Originally certified in January 2019 for up to ASIL D capability
- Re-certified in 2019 for ISO 26262 2nd ed. (published December 2018)



ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

Product Service

CERTIFICATE

No. Q4B 081108 0003 Rev. 01

Holder of Certificate:	NVIDIA Corporation 2701 San Tomas Expressway Santa Clara CA 95050 USA
Factory(ies):	NVIDIA Corporation 2701 San Tomas Expressway, Santa Clara CA 95050, USA
Certification Mark:	ISO 26262
Scope of Certificate:	ECU HW Functional Safety Development Process AUTOFS0001
Applied Standard(s):	ISO 26262-2:2018 ISO 26262-5:2018 ISO 26262-8:2018

The Certification Body of TÜV SÜD Product Service GmbH certifies that the company mentioned above has established and is maintaining a management system which meets the requirements of the listed standards. The results are documented in a report. See also notes overleaf.

Report No.:	NS94580T
Valid until:	2023-01-26

Date, 2020-01-27

(Jiayi Dong)

A4 / 07.17

Page 1 of 1

TÜV SÜD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany

SOFTWARE PROCESS COMPLIANCE

- NVIDIA software process PLC-L3 is applied to all safety-related software projects (including firmware)
- PLC-L3 defines
  - Project lifecycle model from requirements to release
  - Required activities across project lifecycle
  - Independent confirmation measures
- PLC-L3 is developed to comply with
  - ISO 26262:2018
  - ASPICE PAM 3.1

Assessment of PLC-L3 process is in progress with TÜV SÜD

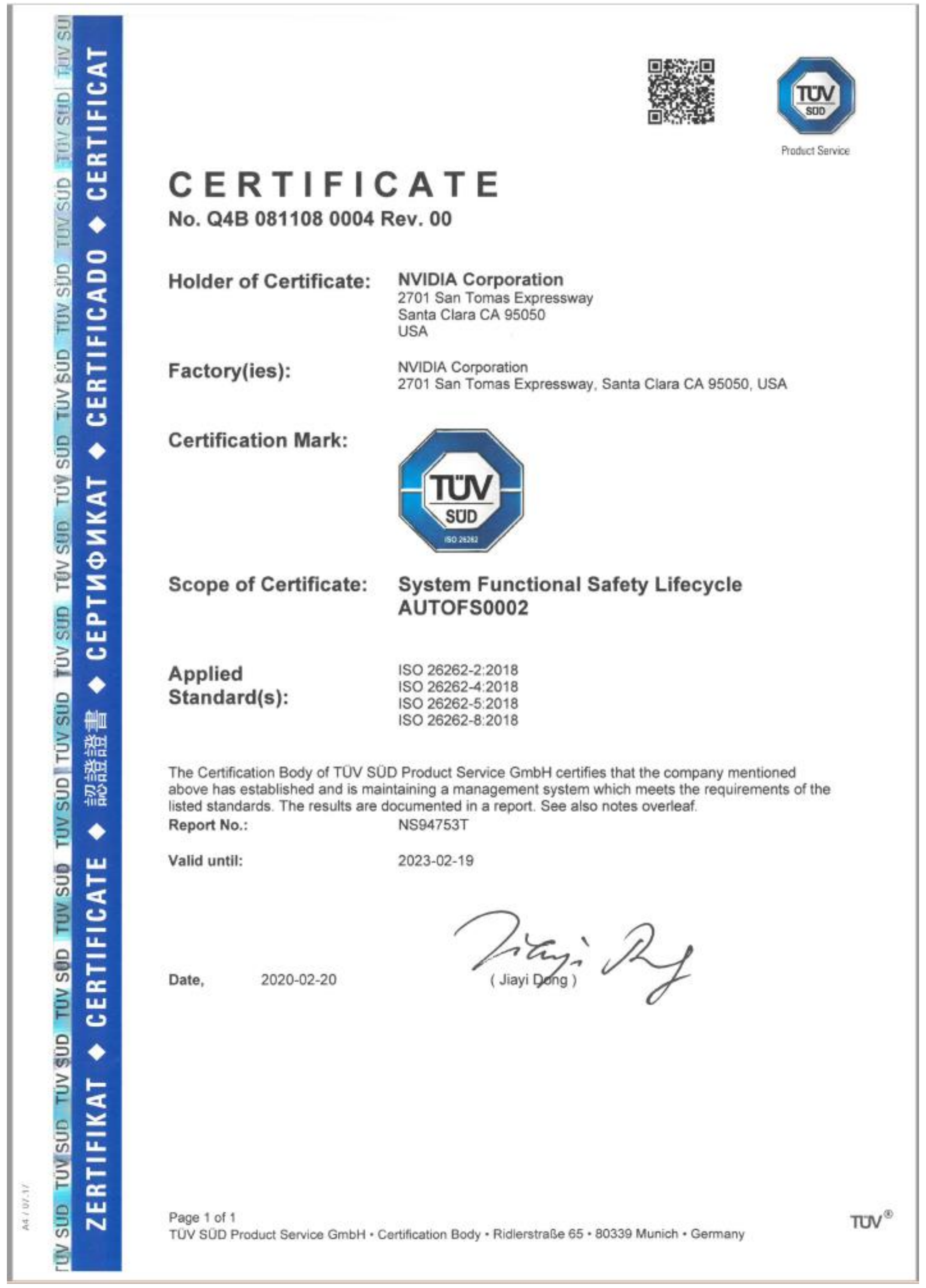
- Process evaluation for up to ASIL D capability
- Expected completion within 2020

SYSTEM PROCESS COMPLIANCE

- Our AUTOFS0002 process provides guidance how to develop ISO 26262 compliant systems which include both HW and SW components

- Being applied to products currently under development

- Originally certified in January 2020 for up to ASIL D capability



ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

Product Service

CERTIFICATE
No. Q4B 081108 0004 Rev. 00

Holder of Certificate: NVIDIA Corporation
2701 San Tomas Expressway
Santa Clara CA 95050
USA

Factory(ies): NVIDIA Corporation
2701 San Tomas Expressway, Santa Clara CA 95050, USA

Certification Mark: TÜV SÜD ISO 26262

Scope of Certificate: System Functional Safety Lifecycle
AUTOFS0002

Applied Standard(s): ISO 26262-2:2018
ISO 26262-4:2018
ISO 26262-5:2018
ISO 26262-8:2018

The Certification Body of TÜV SÜD Product Service GmbH certifies that the company mentioned above has established and is maintaining a management system which meets the requirements of the listed standards. The results are documented in a report. See also notes overleaf.

Report No.: NS94753T

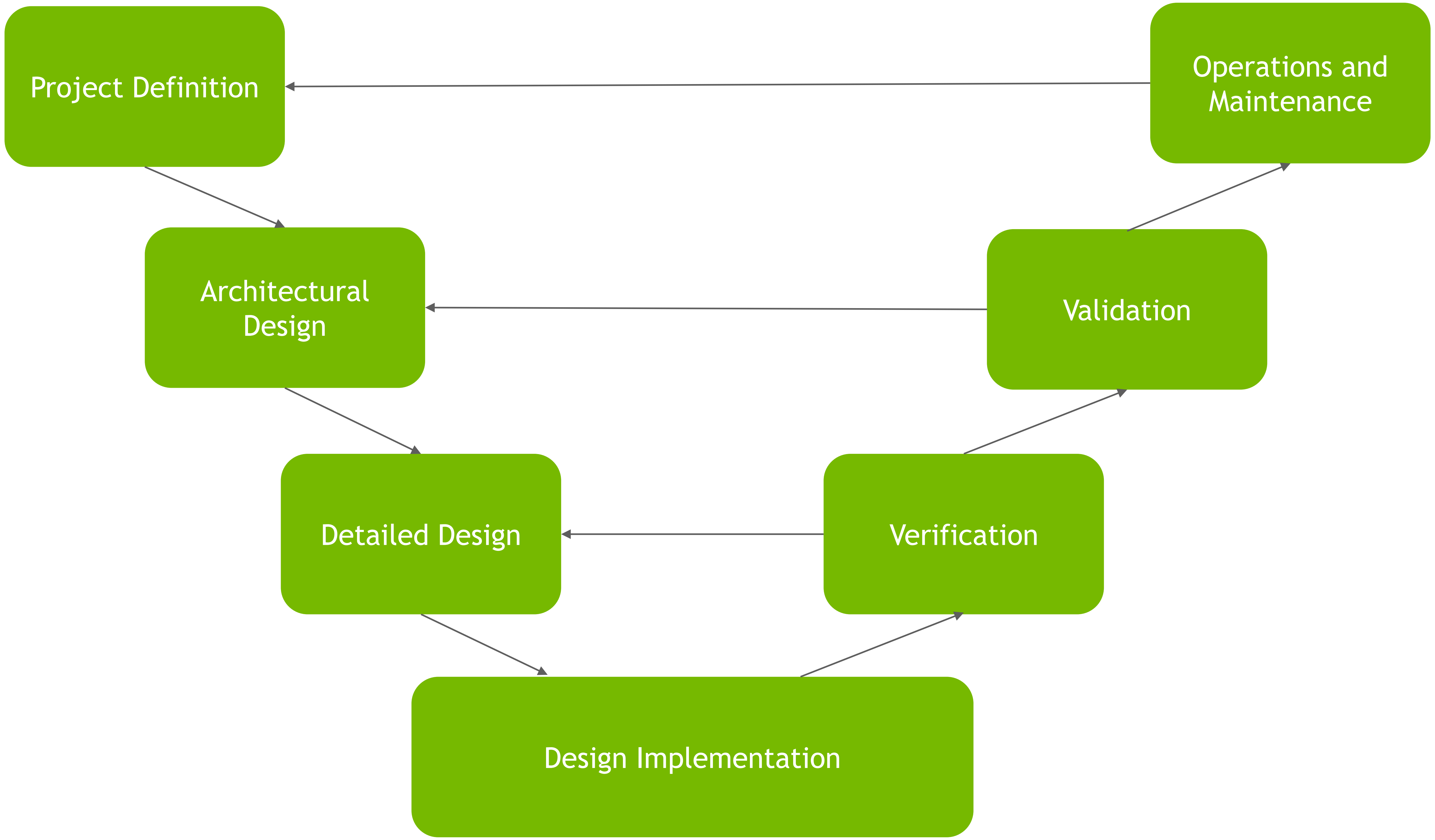
Valid until: 2023-02-19

Date, 2020-02-20

(Jiayi Dong)

Page 1 of 1
TÜV SÜD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany

SIMPLIFIED V MODEL OF DEVELOPMENT



CONCEPT VS. PRODUCT COMPLIANCE

Concept Compliance

- Confirms that a proposed architecture, if implemented properly, should be ISO 26262 compliant
- Focused on left side of V-model
  - Initial product definition and requirements
  - Safety analysis of proposed product
  - Final architectural requirements
  - Design specification

Product Compliance

- Confirms that the implementation of a concept/architecture is compliant to ISO 26262
- Focused primarily on right side of V-model
  - Design execution
  - Design verification
  - Characterization
  - Qualification for production
  - Support for production, operation, and decommissioning

SUCCESSFUL CONCEPT ASSESSMENTS

Date	TÜV SÜD Report	Evaluation target	Target compliance	ASIL
2018-10-05	NS92377T	Xavier T194	ISO 26262-4:2011 ISO 26262-5:2011	C(D)
2019-02-01	NS93571T	Turing TU104	ISO 26262-4:2011 ISO 26262-5:2011	B
2019-03-07	NS93705T	Xavier T194	ISO 26262-4:2011 ISO 26262-5:2011	B

https://www.tuvsud.com/en/e-ssentials-newsletter/rail-essentials/e-ssentials-2-2018/safety-concept-assessment-for-nvidia-xavier-system-on-chip-to-foster-safe-autonomous-driving

SUCCESSFUL PRODUCT ASSESSMENTS

Date	TÜV SÜD Report	Evaluation target	Target compliance	ASIL
2020-05-18	NS95113T	Xavier AD	ISO 26262:2018*	D (systematic) C (random)
2020-05-19	NS95115T	Xavier AD125	ISO 26262:2018*	D (systematic) B (random)
2020-05-19	NS95118T	Xavier T	ISO 26262:2018*	D (systematic) C (random)

* Assessment completed against relevant sections of parts 2, 4, 5, 7, 8, and 9. FW is addressed as part of DRIVE OS product and developed respecting ISO 26262-6.

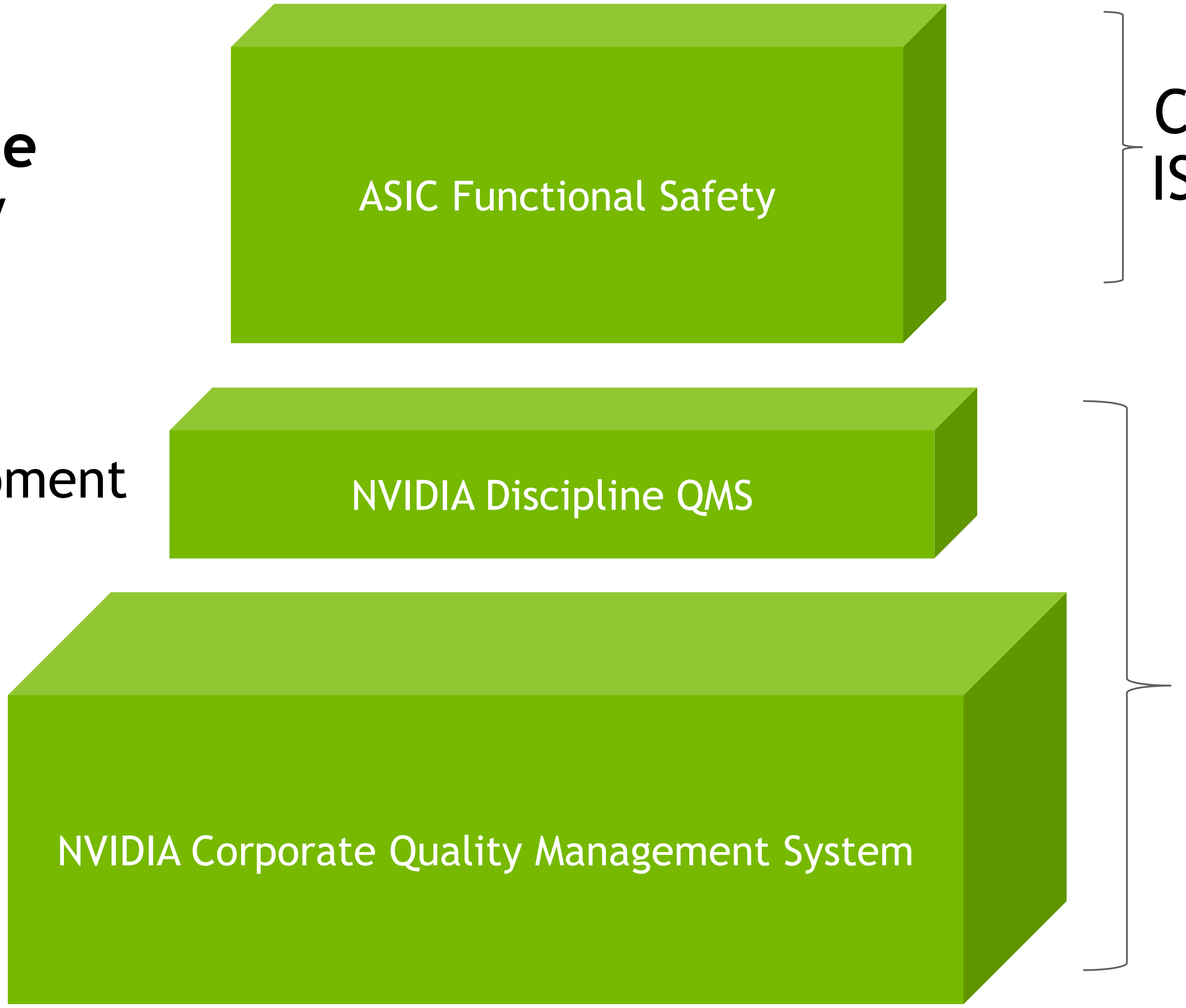
https://www.tuvsud.com/en/e-ssentials-newsletter/rail-essentials/e-ssentials-1-2020/safety-assessment-for-nvidia-xavier-soc-to-foster-safe-autonomous-driving

SOFTWARE ASSESSMENTS

- During 2019-2020 more than 240 internal assessments were completed for the DRIVE OS software elements
- Assessments increase confidence on the correct execution of the PLC-L3 software process and achievement of functional safety
- Every safety-related software program will result in a safety case for the product
    - Explicit claims and arguments for achieved level of functional safety
    - Supported by evidence generated as part of software development activities

NVIDIA PROCESS OVERVIEW

Safety Processes are built on top of Strong Quality Processes



Functional Safety Compliance

- DESIGN0007: ASIC Functional Safety

ASIC Functional Safety

Complies with:
ISO 26262:2018

QMS refinements

- DESIGN0006: ASIC Design & Development

NVIDIA Discipline QMS

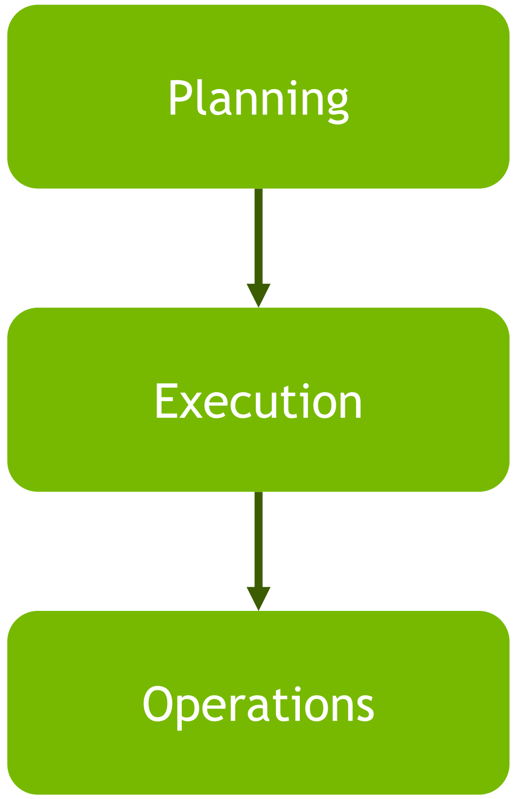
Company Wide
Quality Management System

NVIDIA Corporate Quality Management System

Complies with:
ISO 9001:2015
IATF 16949:2016

DESIGN0007

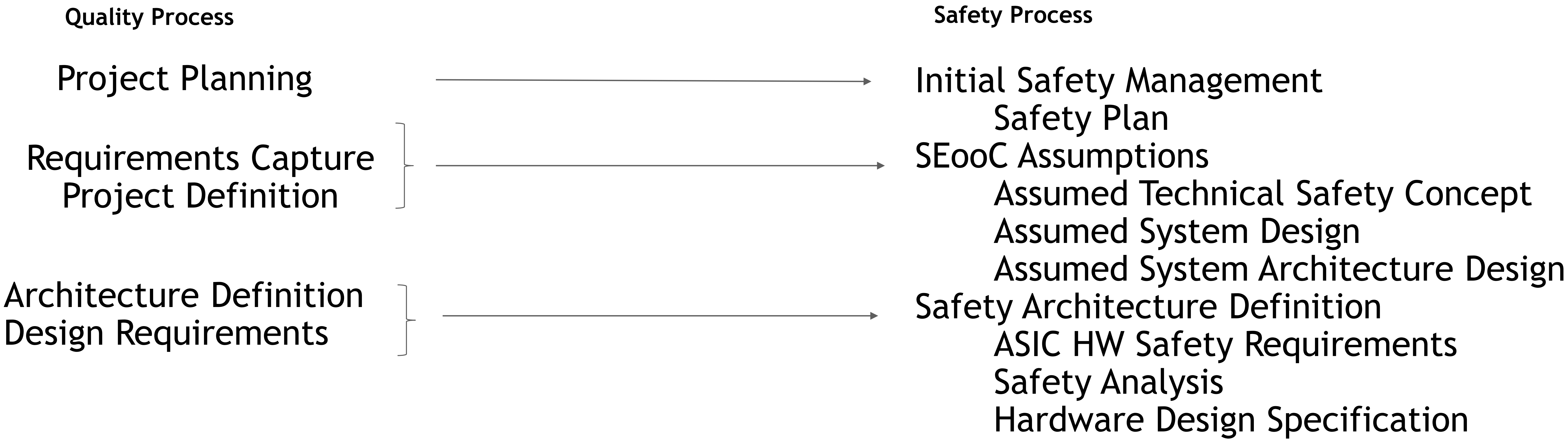
ASIC Safety Lifecycle Phases



- DESIGN0007 can be simplified into three major phases:
  - Design Planning : ISO 26262 Part 2 Management and Part 8 Supporting Processes
  - Design Execution: ISO 26262 Part 5 Hardware Development and Part 9 ASIL Oriented and Safety-Oriented Analyses
  - Operations: ISO 26262 Part 7 Production and Final Safety Case
- Each major phase has sub-phases to simplify project execution and management
- Internal independent audits are conducted at the end of each sub-phase

QUALITY PROCESS FEEDS INTO SAFETY PROCESS

Work Products Aligned at Each Stage of Development



Quality Process

Project Planning

Requirements Capture
Project Definition

Architecture Definition
Design Requirements

Safety Process

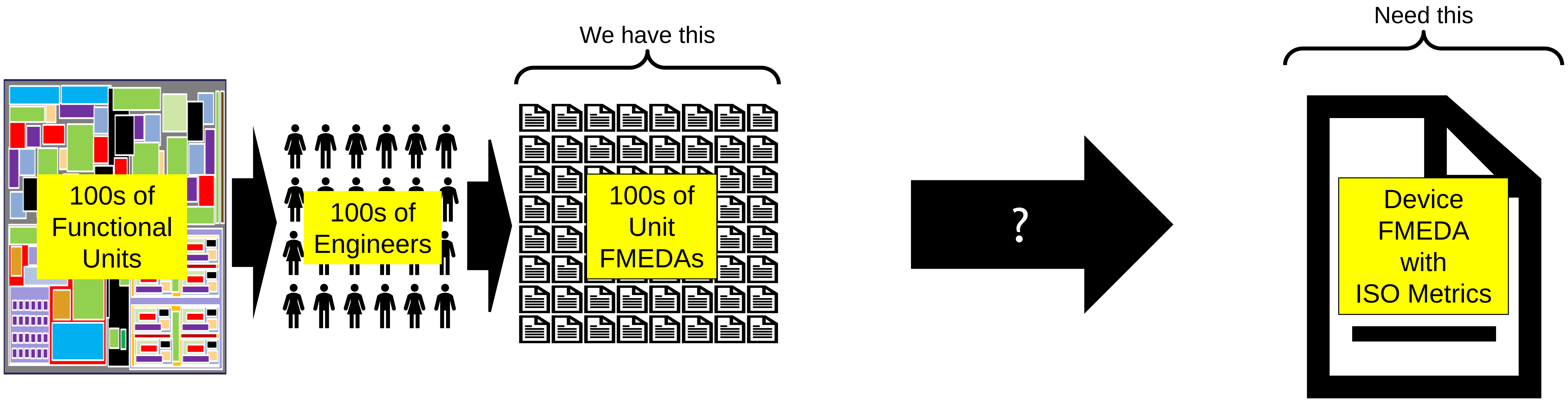
Initial Safety Management
- Safety Plan

SEooC Assumptions
- Assumed Technical Safety Concept
- Assumed System Design
- Assumed System Architecture Design

Safety Architecture Definition
- ASIC HW Safety Requirements
- Safety Analysis
- Hardware Design Specification

TOOLS AND AUTOMATION

VC FSM™ for FMEDA



<u>Challenges</u>

Quality of overall FMEDA with hundreds of authors

Aggregation of 100s of unit FMEDAs into device FMEDA

<u>Solution</u>

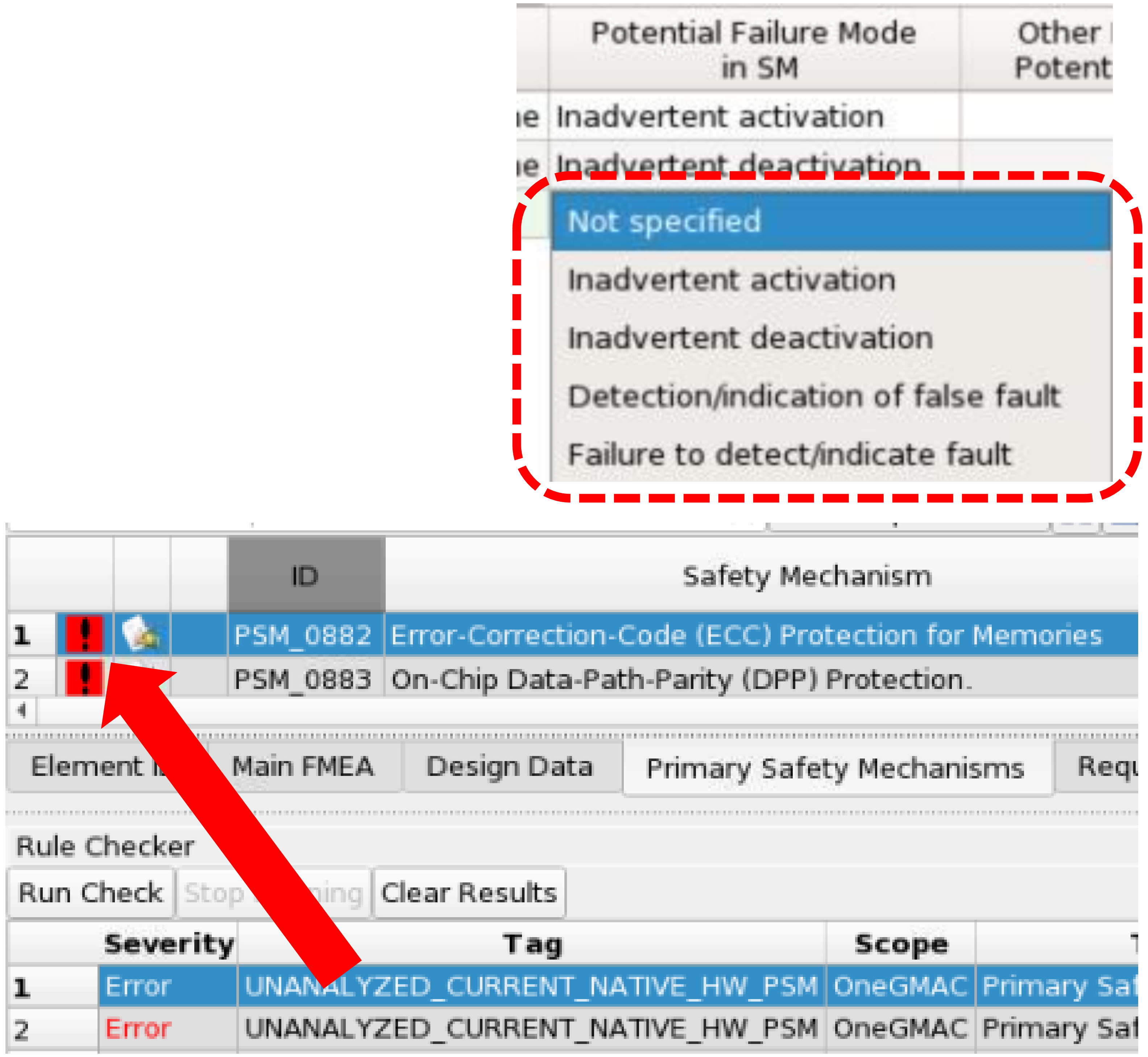
Purpose built tool

VC FSM™ - a collaboration of Synopsys and NVIDIA

TOOLS AND AUTOMATION

VC FSM™ for FMEDA : Distributed, High Quality Analysis

- Device hierarchy specifies how to aggregate unit FMEDAs
- Tool features guide proper user analysis
  - Menus / pick-lists wherever possible
  - Integration with requirements management tool
- Dozens of automated checks
  - All safety mechanisms are full analyzed
  - 100% of failure rate of the unit is accounted for
  - Many, many, more
- NVIDIA developed additional checkers for work products



Potential Failure Mode in SM	Other Potent
Inadvertent activation	
Inadvertent deactivation	

Not specified
Inadvertent activation
Inadvertent deactivation
Detection/indication of false fault
Failure to detect/indicate fault

	ID	Safety Mechanism
1	PSM_0882	Error-Correction-Code (ECC) Protection for Memories
2	PSM_0883	On-Chip Data-Path-Parity (DPP) Protection.

	Severity	Tag	Scope	T
1	Error	UNANALYZED_CURRENT_NATIVE_HW_PSM	OneGMAC	Primary Saf
2	Error	UNANALYZED_CURRENT_NATIVE_HW_PSM	OneGMAC	Primary Saf

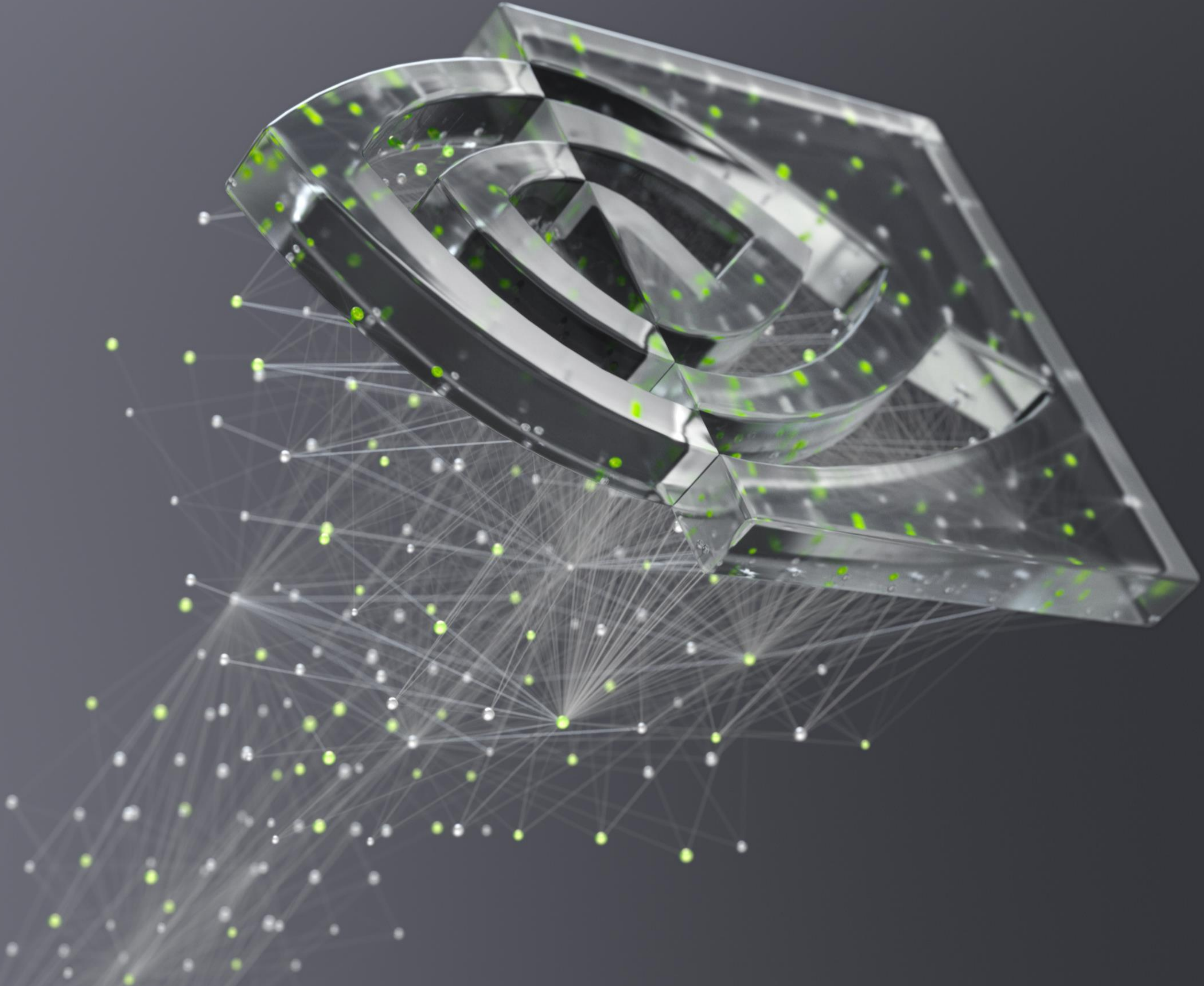
FAULT INJECTION CHALLENGES

- The performance of implemented safety mechanisms must be verified – typically through fault injection simulation
    - On a complex SoC like Xavier, there are trillions of possible faults that could be simulated.
    - But, current state of the art tools can only simulate millions of faults.

- Xavier required new methodologies for fault injection:
    - Sampling techniques to reduce the fault list down to thousands
    - Analysis techniques to prioritize faults that are the most likely to be dangerous
    - Architectural reuse of common safety mechanisms

NVIDIA’S SAFETY EFFORT

- Large, multi-year investment in safety for autonomous vehicles
- Investing in a full stack solution – hardware, software, systems, and tools
- Complexity exceeds traditional safety systems, requiring new approaches to process, methodology, and tools
- Requires high effort and extraordinary patience – investments started in 2014
- Continuously improving over multiple generations



NVIDIA