Diverse Redundancy & Testability: Key Drivers for Intelligent Vehicle Dependability

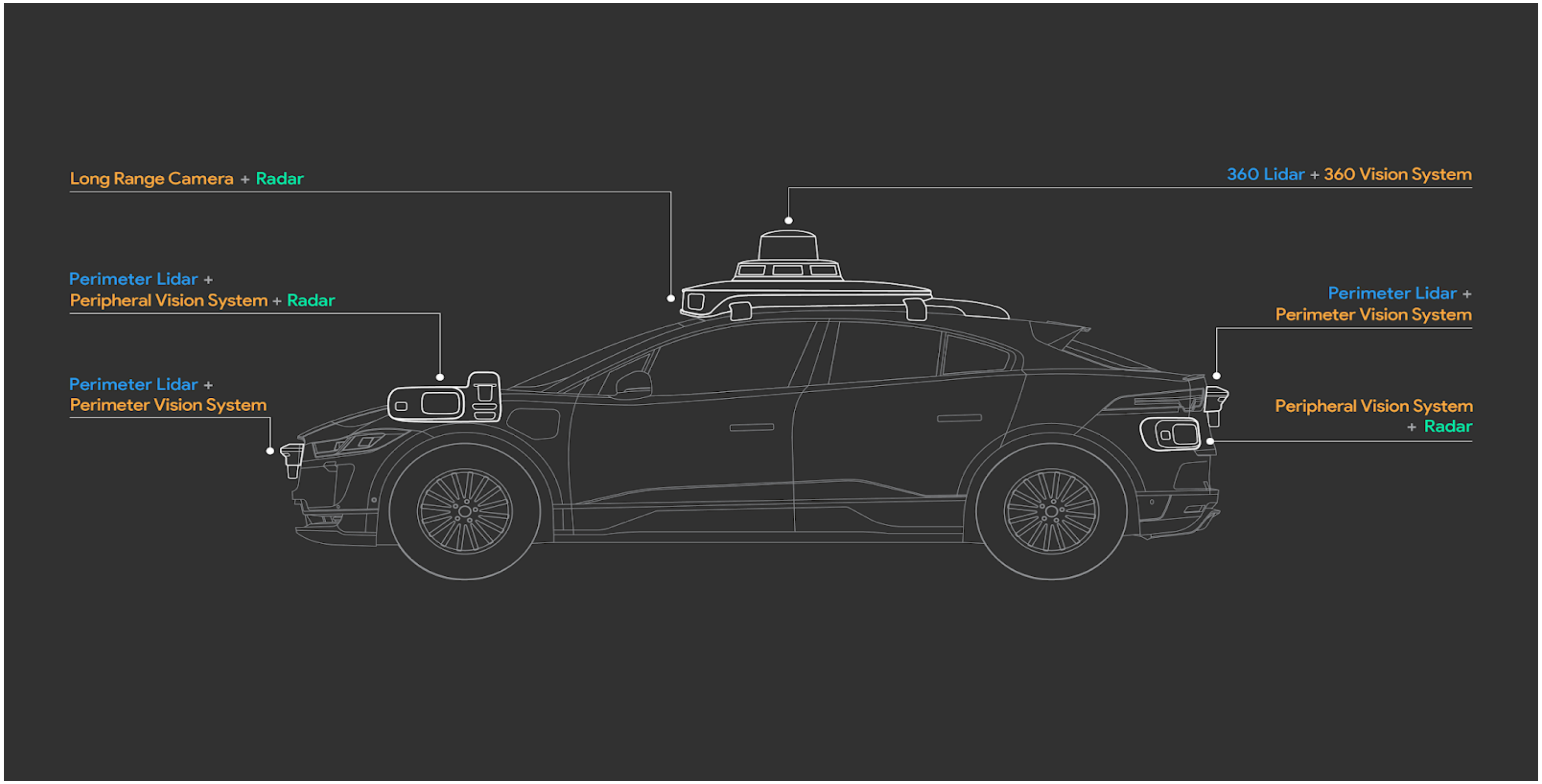
Nirmal R. Saxena
NVIDIA
Jan 30, 2021

NVIDIA

Storyline

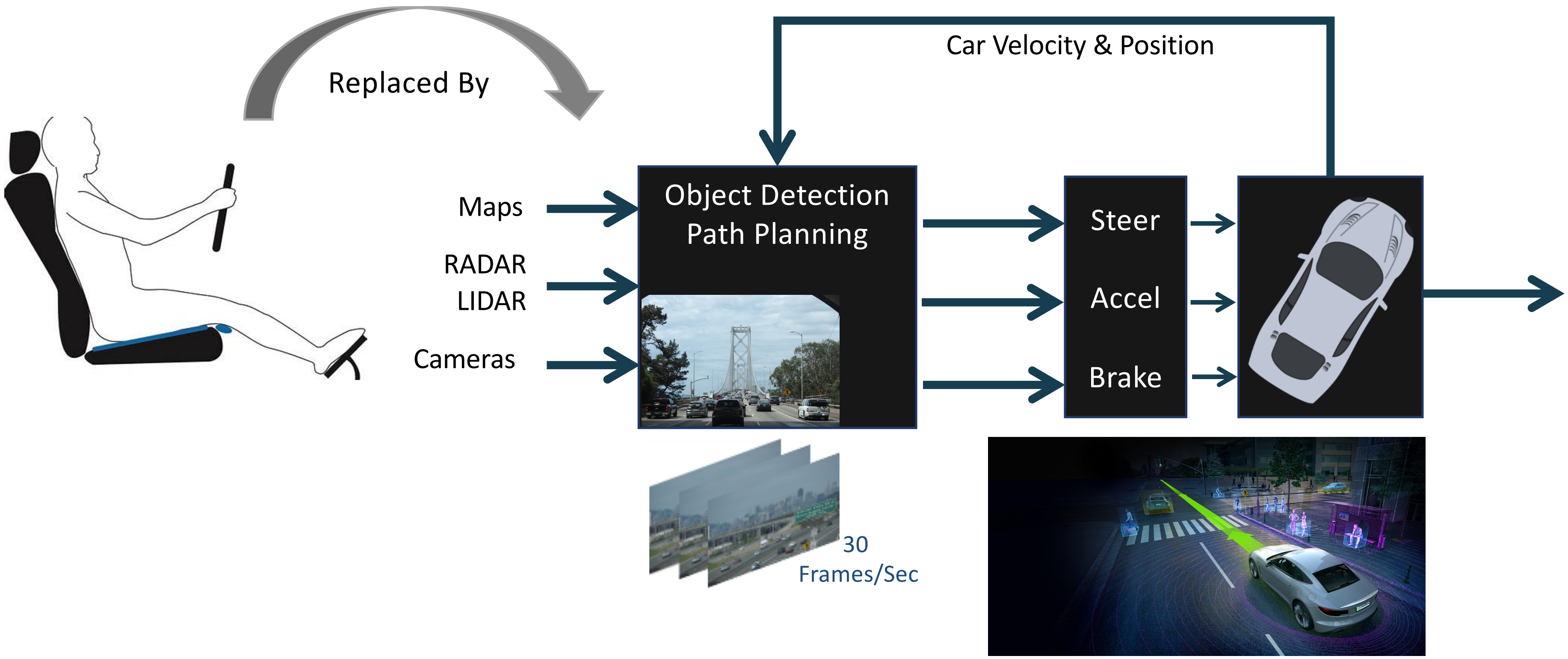
- Intelligent Car Model
- Auto Safety Standard
  - Safety Targets vs. Accident Metrics
- Testability
  - DL Accuracy vs. Safety
  - Systematic Faults & Validation
  - Transient & Permanent Faults
- Diverse Redundancy
  - Reliability Models
  - Need for Diversity– Systematic Faults

Cameras & Sensors in an Intelligent Vehicle

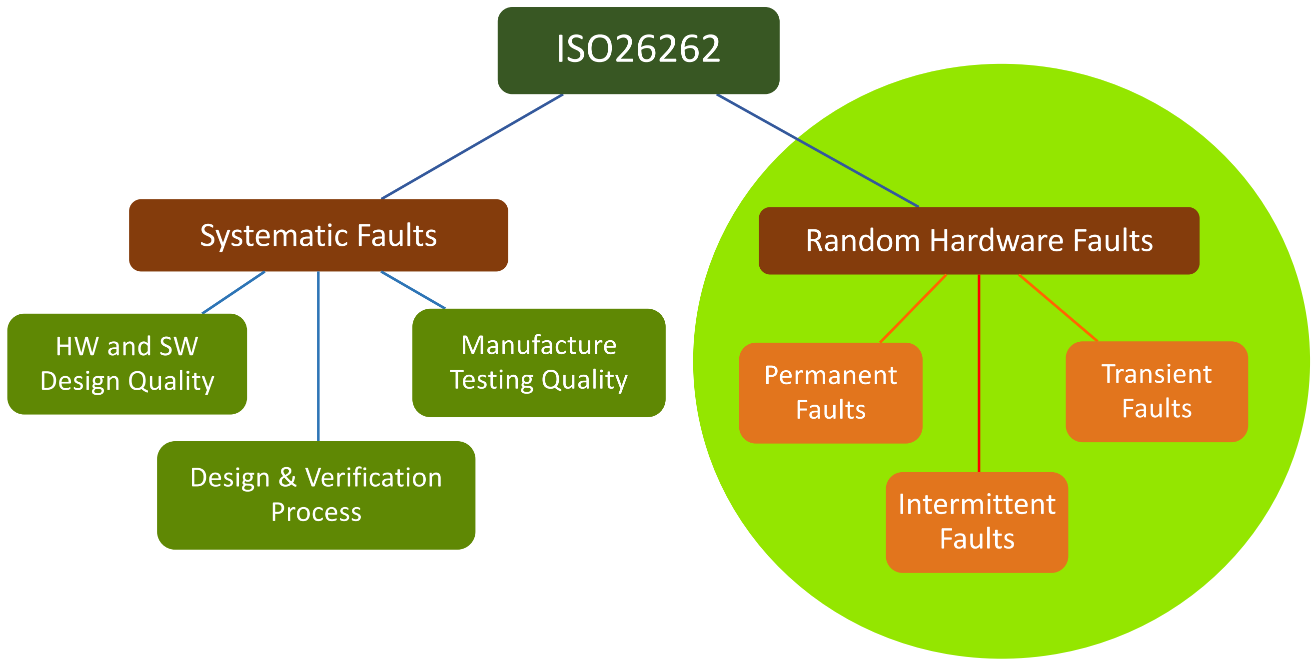


Source: Waypoint - The official Waymo blog: Introducing the 5th-generation Waymo Driver: Informed by experience, designed for scale, engineered to tackle more environments

Control System Model– Intelligent Car



ISO26262 Auto Safety Specification

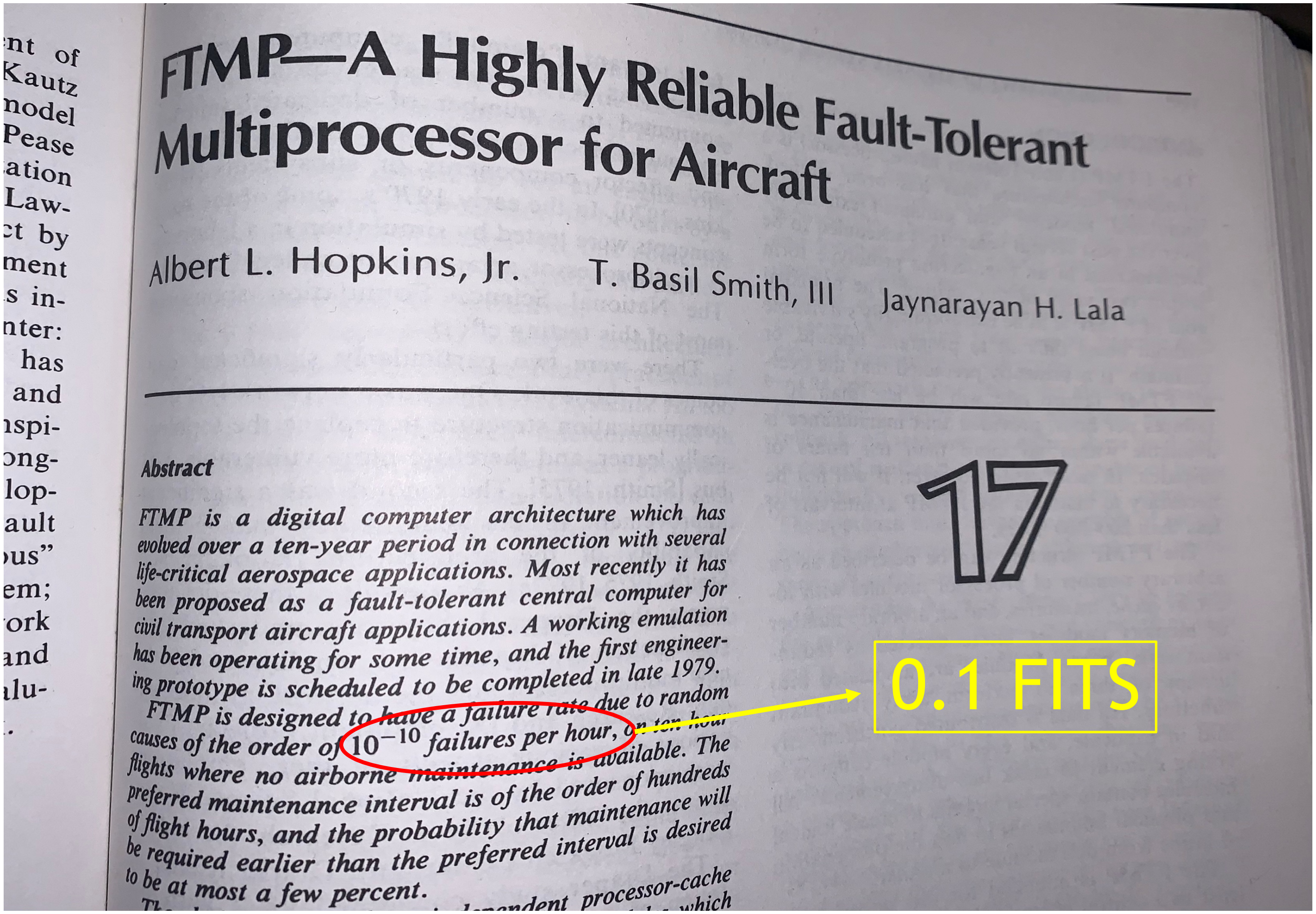


Random Hardware Faults Targets

Hardware Random Fault Metrics	ASIL B	ASIL C	ASIL D
Permanent Fault Coverage (SPFM)	90%	97%	99%
Transient Fault Coverage (SPFM)	90%	97%	99%
Latent Fault Coverage (LFM)	60%	80%	90%
Hardware Failure Probability (PMHF)	100FIT $\leq 10^{-7}/hr$	100FIT $\leq 10^{-7}/hr$	10FIT $\leq 10^{-8}/hr$

FIT = Failures in Time, Time = 10^9 Hours. 1 FIT = 10^{-9} *failures/hour*

ASIL	Automotive Safety Integrity Level
SPFM	Single Point Fault Metric
LFM	Latent Fault Metric
PMHF	Probabilistic Metric for Hardware Failures



FTMP—A Highly Reliable Fault-Tolerant Multiprocessor for Aircraft

Albert L. Hopkins, Jr. T. Basil Smith, III Jaynarayan H. Lala

17

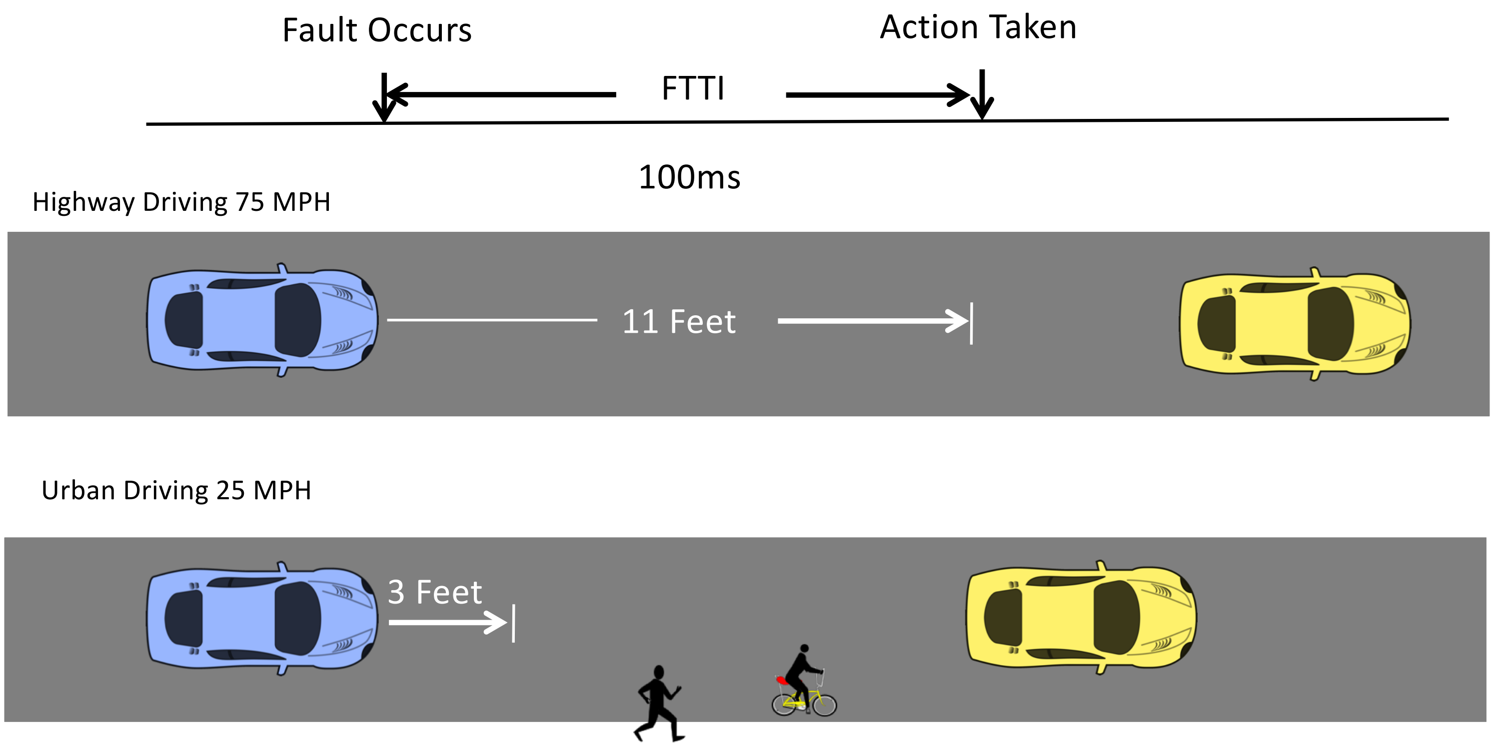
Abstract

FTMP is a digital computer architecture which has evolved over a ten-year period in connection with several life-critical aerospace applications. Most recently it has been proposed as a fault-tolerant central computer for civil transport aircraft applications. A working emulation has been operating for some time, and the first engineering prototype is scheduled to be completed in late 1979.

FTMP is designed to have a failure rate due to random causes of the order of 10^{-10} *failures per hour, on ten hour flights where no airborne maintenance is available. The preferred maintenance interval is of the order of hundreds of flight hours, and the probability that maintenance will be required earlier than the preferred interval is desired to be at most a few percent.*

Book- The Theory and Practice of Reliable System Design, Daniel P. Siewiorek & Robert S. Swartz

Fault Tolerant Time Interval (FTTI)



Accident Statistics– US

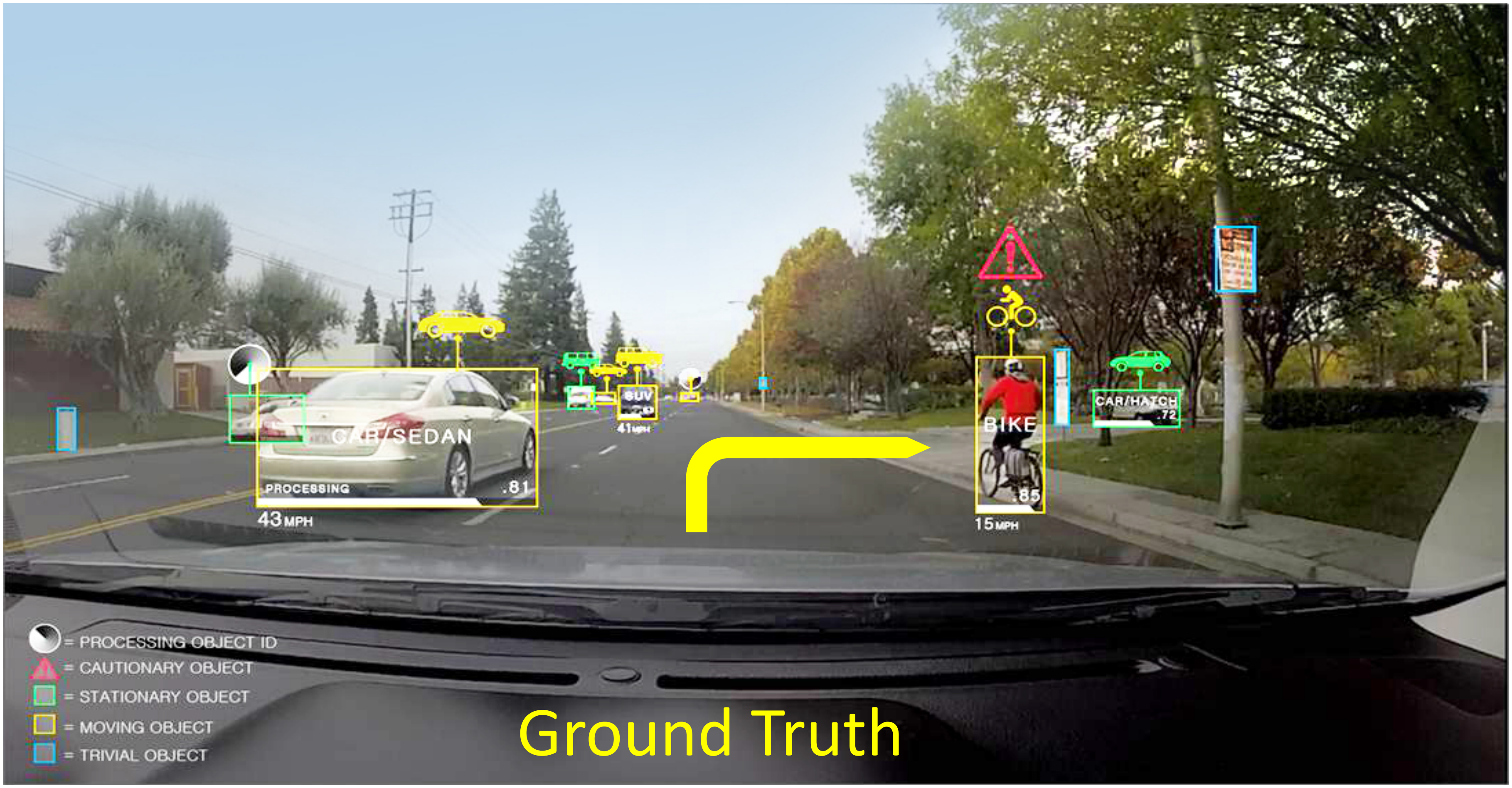
Reference: National Highway Traffic Safety Administration (NHTSA): www.nhtsa.gov

Description	2013 Statistics	2015 Statistics
Fatal Crashes	30,057	35,092
Driver Related Fatal Crashes	10,076	10,265
Non-Fatal Crashes	5,657,000	6,263,834
Number of Registered Vehicles	269,294,000	281,312,446
Licensed Drivers	212,160,000	218,084,465
Vehicle Miles Travelled	2,988,000,000,000	3,095,373,000,000
Fatal Crash Rate in FITs	250 – 500	283 - 566
Non-Fatal Crash Rate in FITs	46K – 92K	51K – 102K
ASIL D 10 FITs is ~ 50x Improvement over Fatal Crash Rate & 4 Orders of Improvement in Non-Fatal CR FITs		

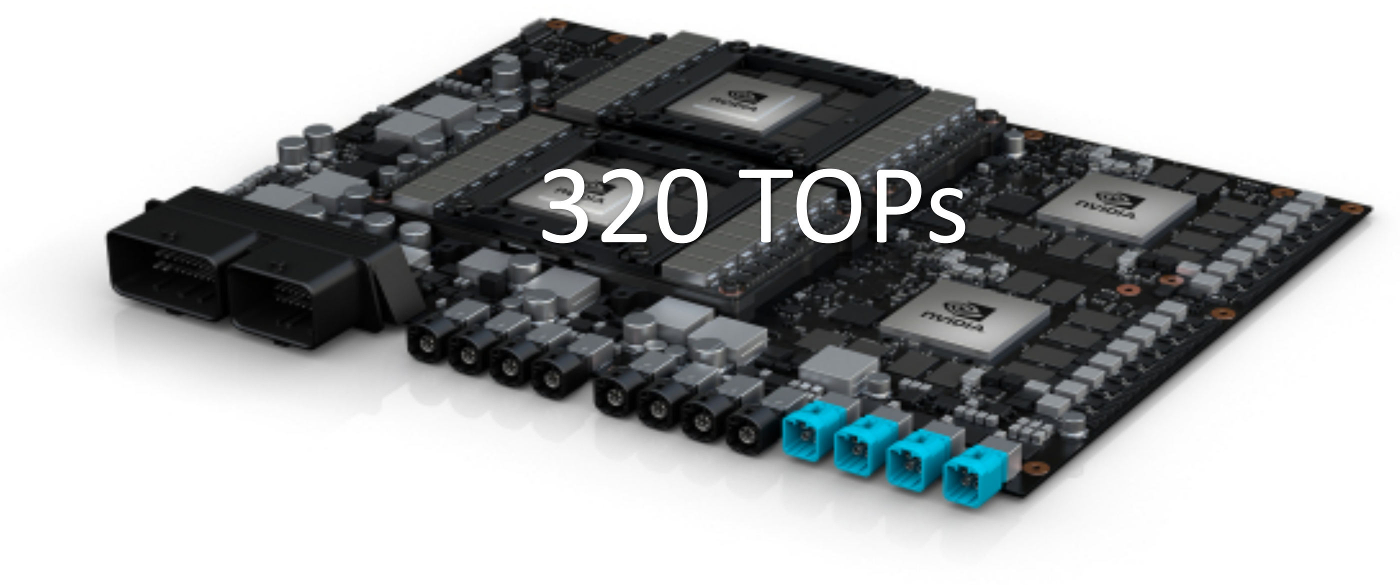
Economic Cost of Traffic Crashes (2010) $242 Billion

Published AV Non-Fatal Crash FIT Rate = 150K

Object Detection & Path Planning– Contextual Accuracy



Object Detection, Path Planning & Other AI Functions Need Enormous Computational Power



https://www.anandtech.com/show/11913/nvidia-announces-drive-px-pegasus-at-gtc-europe-2017-feat-nextgen-gpus

Compute Workload : Perception

Perception Challenge : Achieve "perfect" Object Detection Accuracy

Deep Learning = State of the Art Method

Detection Accuracy & Systematic Faults (SW Bugs)

- When does Detection Accuracy Matter?
  - Traffic Light Detection: Red, Green & Orange (100%)
  - Objects in and around Path Plan (100%)
  - Distant Objects Not in Path Plan (0%)
- Validation of SW & Drive System Software Stack
  - Augmented Virtual Reality
  - Evaluate Millions of Scenarios
  - Simulate Millions-of-Miles-Traveled in a Day
    - Use Massively Parallel Super Computers
  - Dangerous Scenarios with No Physical Harm
  - ➢ Compute for Safety

Nvidia DRIVE Constellation in Datacenters

Transient Fault Injection

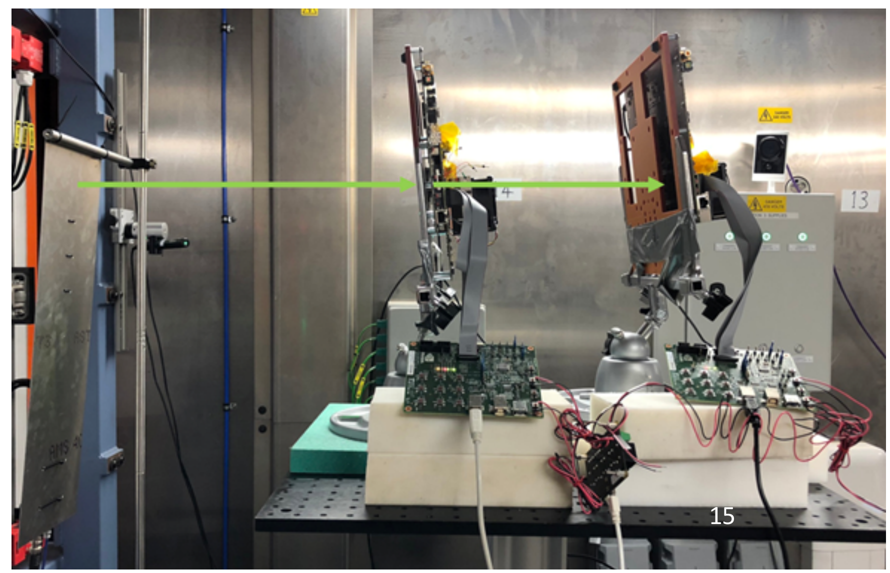
Accelerated Neutron Beam Testing

- Radiation experiments beam testing campaigns
  - Weapons Neutrons Research @ LANSCE
  - ChipIR microelectronics @ Rutherford Appleton Laboratory
- 2000 years of exposure to terrestrial neutron flux

- Experiment Design

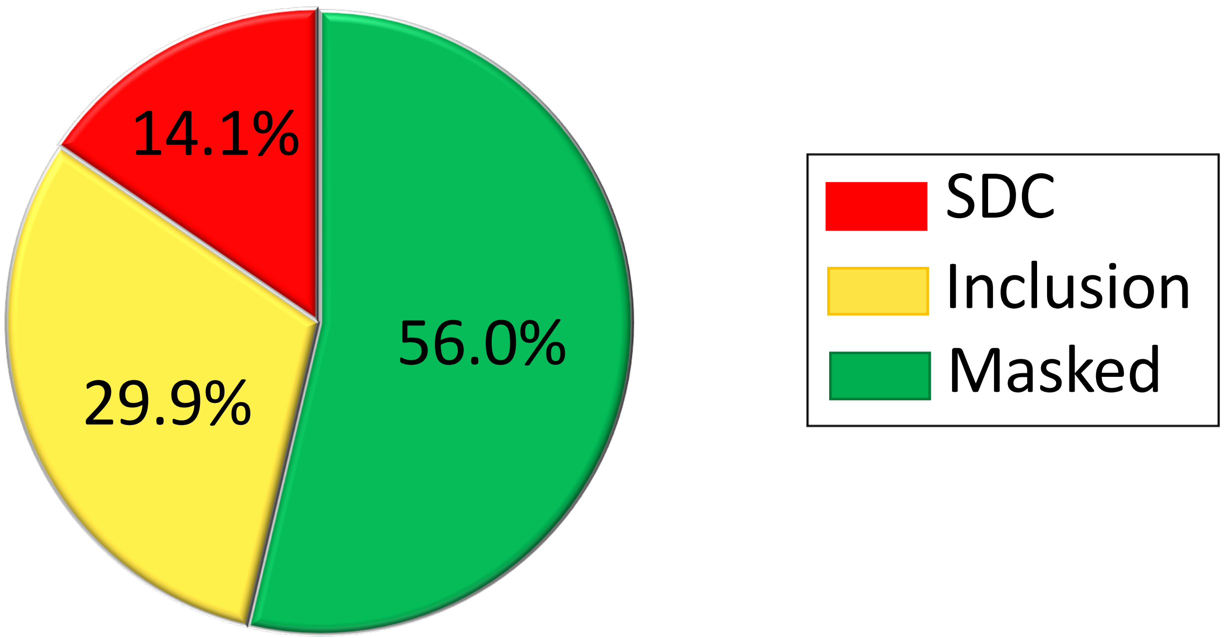
DRAM ECC	SRAM ECC
OFF	OFF
ON	OFF
ON	ON

Flight path of neutron beam



Accelerated Beam Testing Results

DRAM ECC	SRAM ECC
OFF	OFF



SDC: Silent Data Corruption

Accelerated Beam Testing Results

DRAM ECC	SRAM ECC
ON	ON

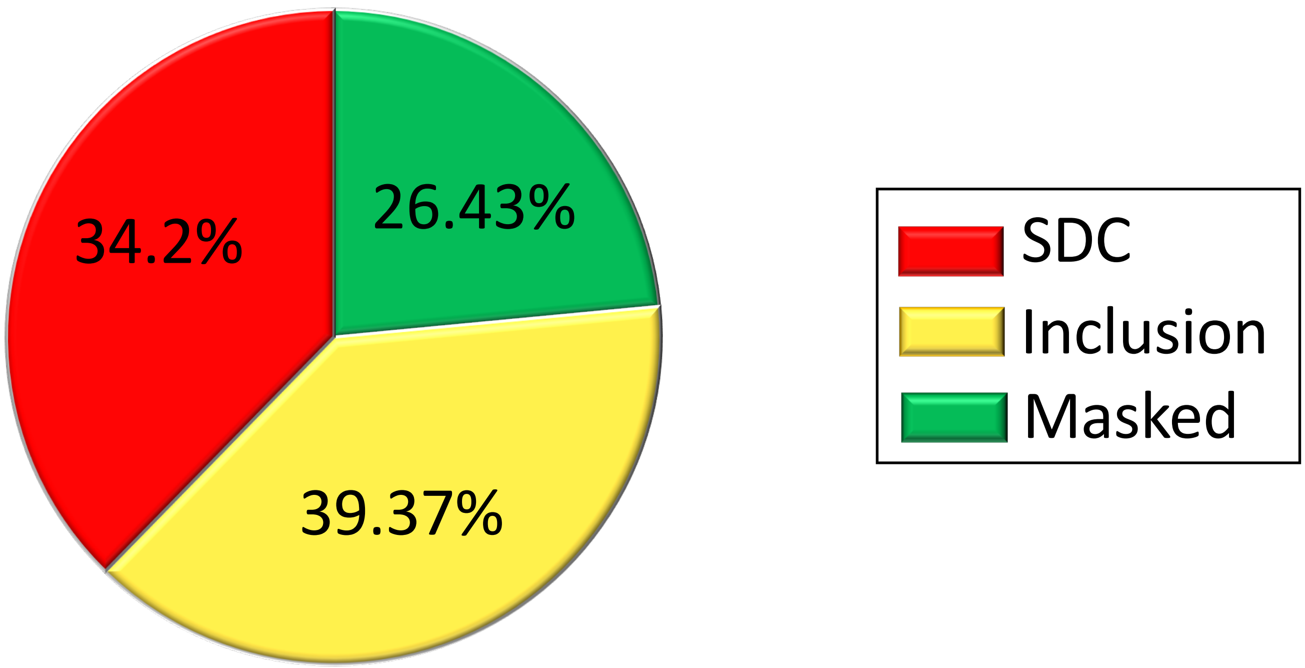
Masked
or
Detected

Zero SDC Events

Permanent Fault Injection

Permanent Fault Injection Results

- Faults in input batches: SDC (+ inclusion) < 1.8%
- Faults in weights:



Object detection networks are vulnerable to permanent faults

Object Detection Conclusion

- Without protection– object detection networks show high SDC rate
  - Unlike classification networks that show resilience to transient errors
- Zero SDC with chip-level protections
  - For transient faults
- Not all permanent fault are detected by ECC/Parity:
  - Raw permanent FIT rate (hundreds) vs raw transient FIT rate (tens of thousands)
    - Offline structural tests during key-off and key-on events,
    - Online periodic tests (meeting FTTI requirement)

Road to Resiliency

Markov Chain Analysis– Need Physical Redundancy

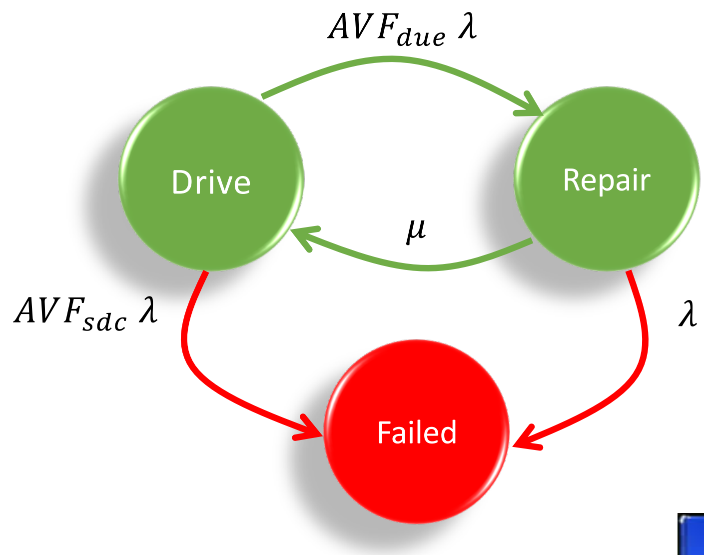
Availability is Important Here

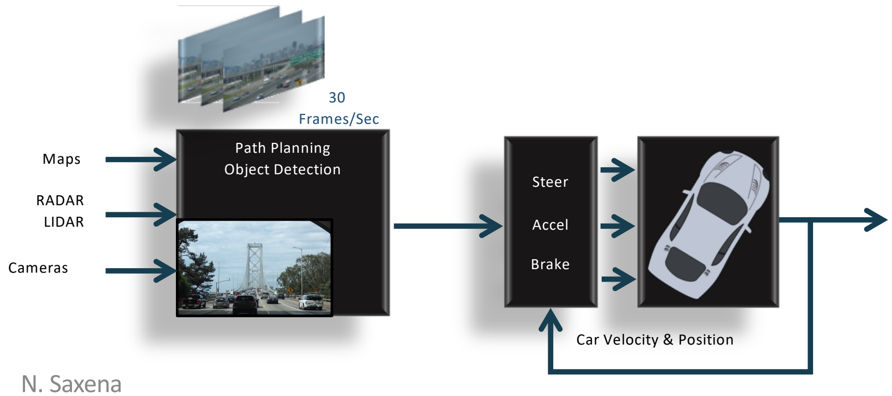
For Driverless Car

Loss of Frames => Loss of Life

For 3 Frame-Tolerance, Need

$$\frac{1}{\mu} < 100ms$$





Dual Redundant System

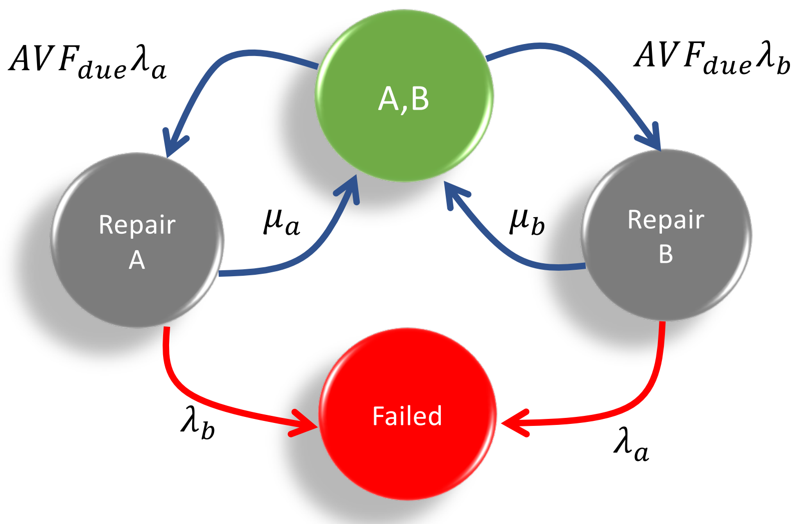
Relaxed Constraints on Repair Rate

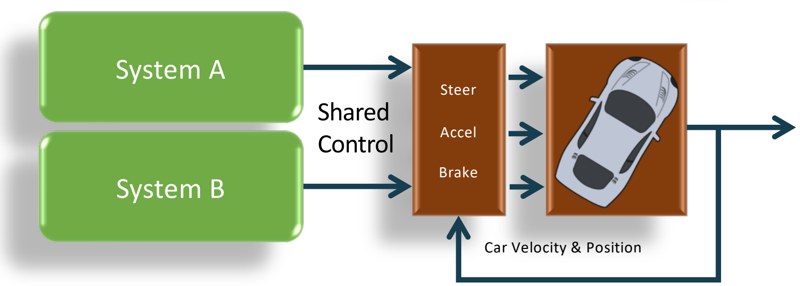
$$\frac{1}{\mu_a} < \frac{1}{\lambda_b}$$

$$\frac{1}{\mu_b} < \frac{1}{\lambda_a}$$

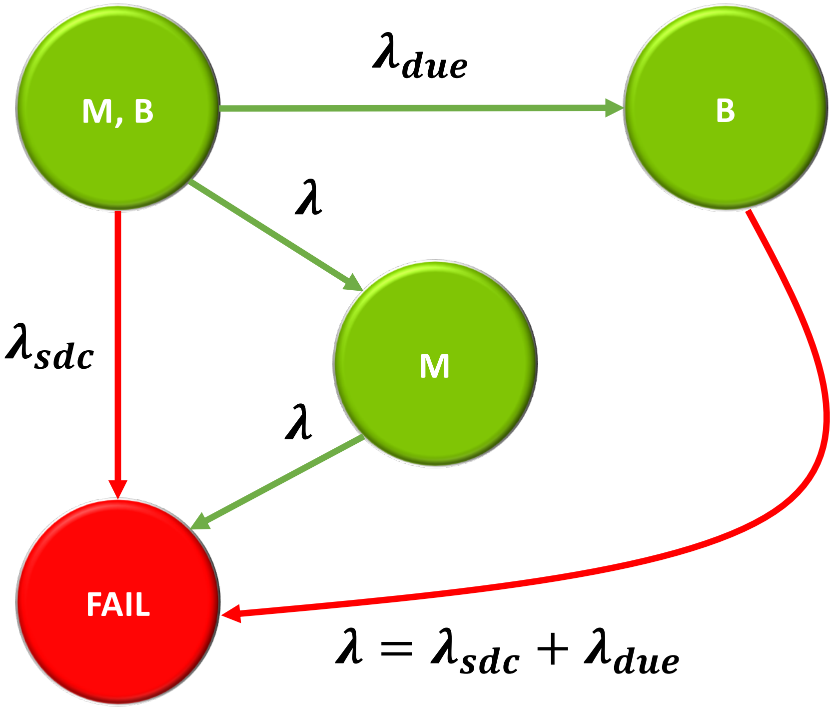
$\frac{1}{\lambda_a}$ or $\frac{1}{\lambda_b}$ in the order 1000's of hours

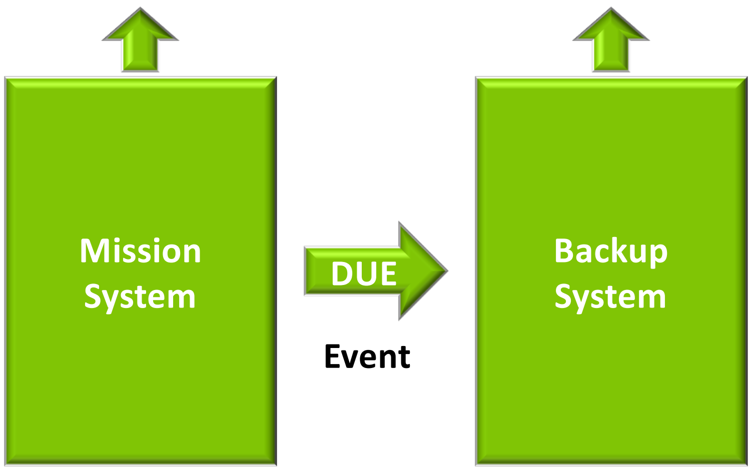
Repair can wait till the next Key-Off Event





Backup Standby Model– Markov Chain





N. Saxena

Probability of Backup Markov Chain States

$$Probability\ of\ being\ in\ M, B\ state, P_{m,b}(t) = e^{-2\lambda t}$$

$$Probability\ of\ being\ in\ B\ state, P_b(t) = \frac{\lambda_{due}}{\lambda}\left(e^{-\lambda t} - e^{-2\lambda t}\right)$$

$$Probability\ of\ being\ in\ M\ state, P_m(t) = e^{-\lambda t} - e^{-2\lambda t}$$

$$Probability\ of\ being\ in\ Fail\ State, F(t) = 1 - \left(\frac{\lambda + \lambda_{due}}{\lambda}\right)e^{-\lambda t} + \frac{\lambda_{due}}{\lambda}e^{-2\lambda t}$$

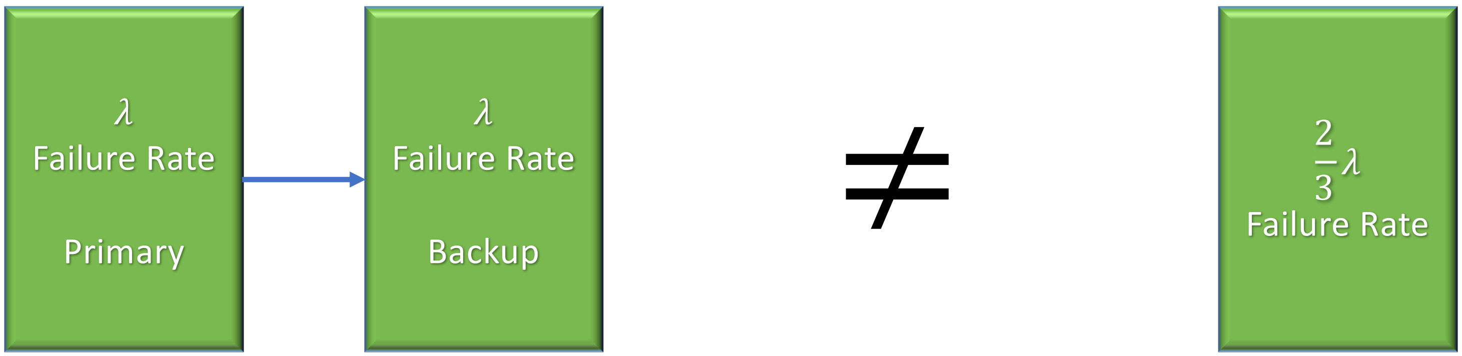
$$\boldsymbol{MTTF = \int_0^\infty t\frac{dF(t)}{dt}dt = \frac{1}{\lambda} + \frac{\lambda_{due}}{2\lambda^2}\ asymtotically\ approaches\ \frac{3}{2\lambda}\ (when\ \lambda_{sdc} = 0)}$$

1.5x Gain in MTTF over Simplex or 1.5x Reduction in Effective Failure Rate over an infinite drive time

N. Saxena

Is MTTF Sufficient to Distinguish Two Systems?

Duplex System | Simplex System

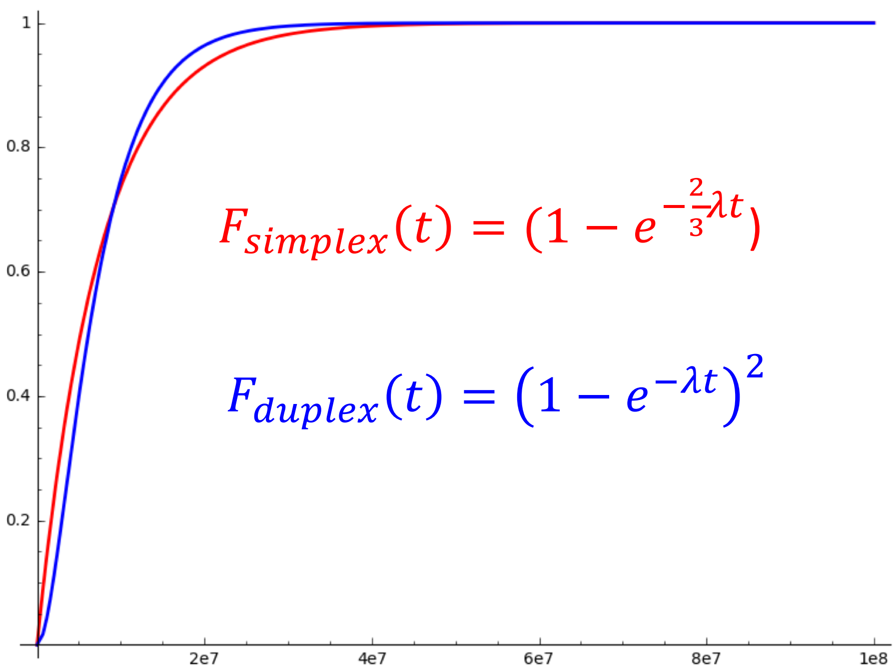


$$Duplex\ MTTF = \frac{3}{2}\lambda$$

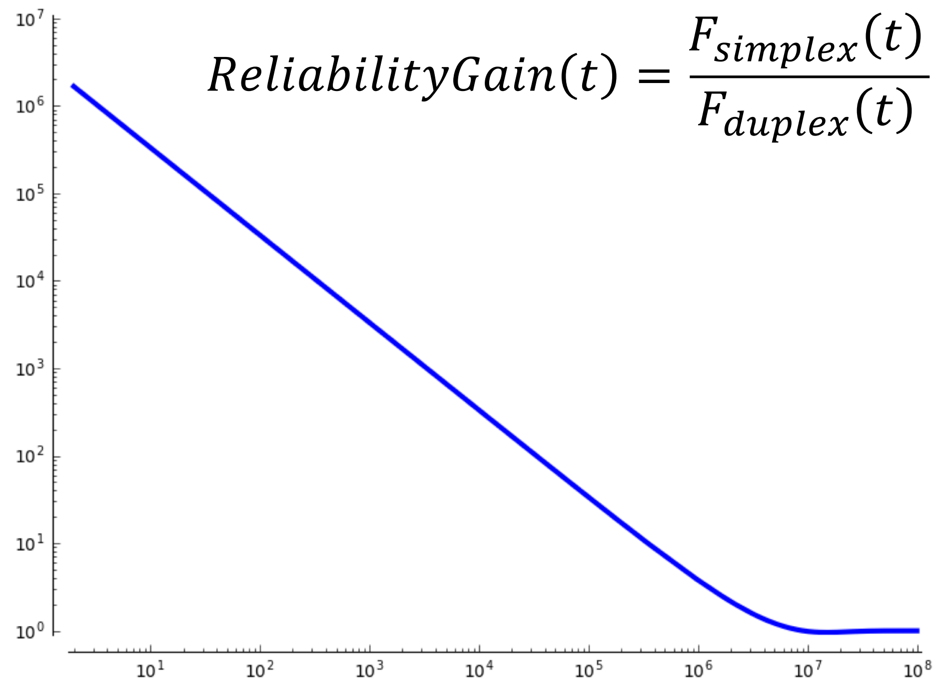
$$Simplex\ MTTF = \frac{3}{2}\lambda$$

Failure Probability Reduction metric as a function of mission time distinguishes various redundant systems [Mitra, Saxena, McCluskey 2004].
S. Mitra, N.R. Saxena, and E.J. McCluskey, "Efficient Design Diversity Estimation for Combinational Circuits," *IEEE Trans. Comp.*, Vol. 53, Issue 11, pp. 1,483-1,492, Nov. 2004
S. Mitra, N.R. Saxena and E.J. McCluskey, "Common-Mode Failures in Redundant VLSI Systems: A Survey," *IEEE Trans. Reliability*, Special Issue on Fault-Tolerant VLSI Systems, Vol. 49, Issue 3, pp. 285-295, Sept. 2000.

Reliability Gain with Perfect Duplex
$\times 10^6$ *in 2 Hour Drive Time*



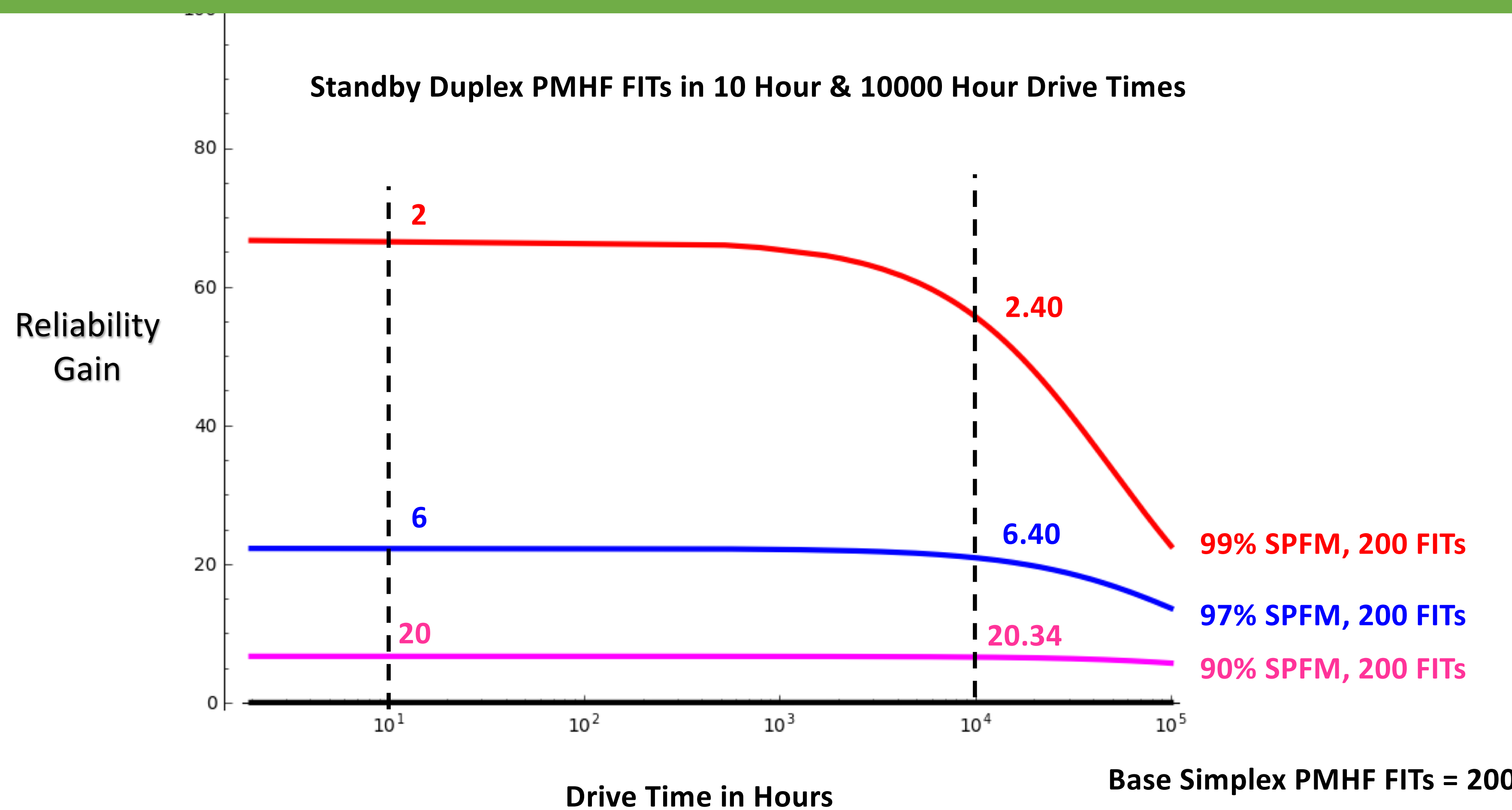
Drive Time in Hours



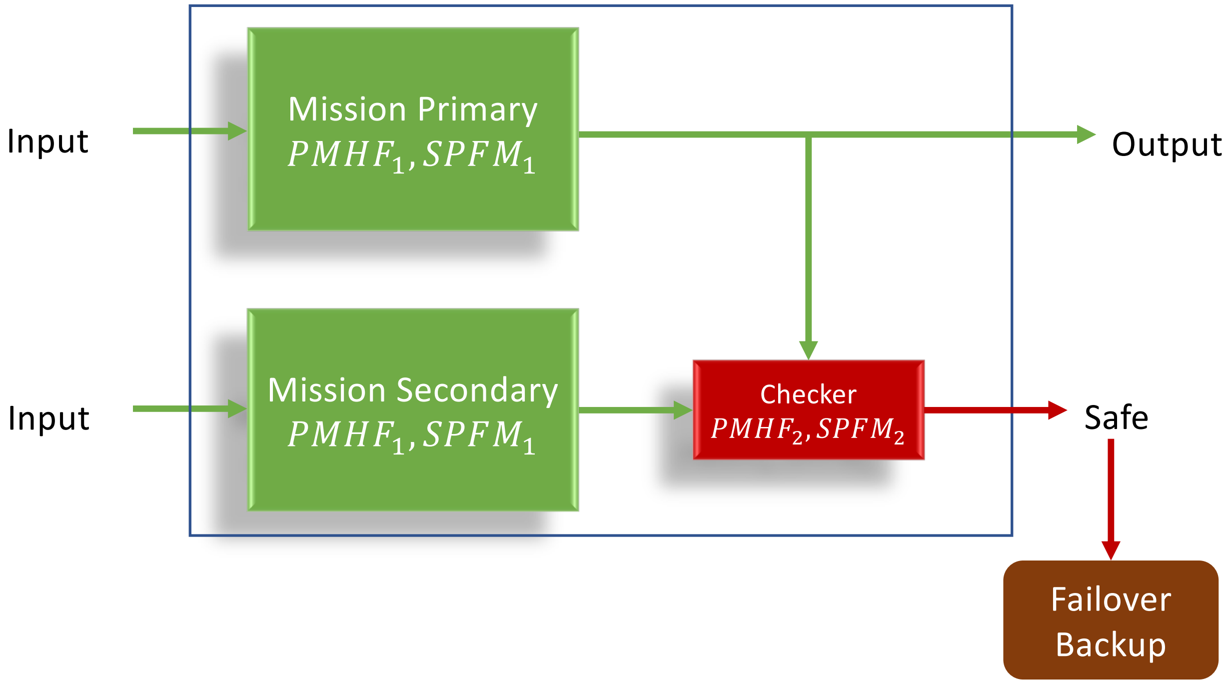
Drive Time in Hours

$$\lambda = 200\ FITs$$

Back-Up Standby Model– SPFM Sensitivity

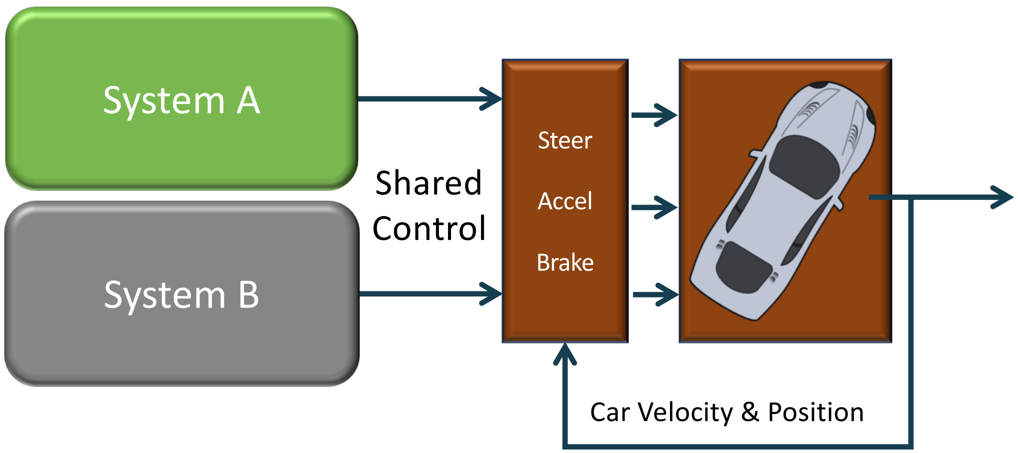


Duplex System with Decoupled Checker



Duplex System PMHF largely Independent of SPFM of Mission Primary or Secondary System

Design Diversity



Coping with Systematic Hardware and Software Design Errors

- [Siewiorek et. al. 1978] (byte reversal copies C.mmp processor)
- [Sedmak and Liebergot 1980] (complementary function diversity in VLSI)
- [Chen and Avizienis 1978] (N-version programming, SIFT software implemented fault-tolerance)
- [Horning et. al 1974] (Recovery Blocks) [Patel] RESO Technique
- [Amman and Knight 1987] (Data Diversity)
- [McCluskey, Saxena, Mitra 1998] Diversity for Reconfigurable Logic & Quantifying Diversity

Conclusions

Road to Resiliency $\Rightarrow$ Dual Redundancy or Graceful Degradation

- Mitigates Permanent Fault Testing
- Higher Availability During Mission Critical Time (Drive Time)

Systematic Faults

- Rigorous Testing and Validation
  - Need 3-to-4 Orders of Improvement
- Physical Redundancy with Design Diversity