The Evolution and Future of Safety

Core Avionics & Industrial Inc.
a Channel One company

Safety Critical Platforms
Lee Melatti

www.coreavi.com


2017 Was The Safest Year In The History Of Air Travel
Airliner accident fatalities by year from 1972 to 2017*
2,500
2,000
1,500
1,000
500
0
2,379
59
'72
1980
1990
2000
2010
'17
* Accidents excluding suicide, sabotage, hijackings etc.
@StatistaCharts
Source: Aviation Safety Network
Forbes
statista

COREAVI

Aviation Safety

- It is estimated that 40 million commercial flights will occur worldwide in 2019
- The fatal accident rate for large commercial passenger flights in 2018 was 0.36 per million flights, or one fatal accident for every 3m flights
- That is up from 2017's 0.06 per million flight rate and above the most recent five-year average of 0.24 per million flights
- Recent B737 Max 8 events underscore the need for safety certification process, oversite and, most importantly, culture
- Safety events trigger large scale investigations that typically result in broad safety modifications and industry improvements

COREAVI

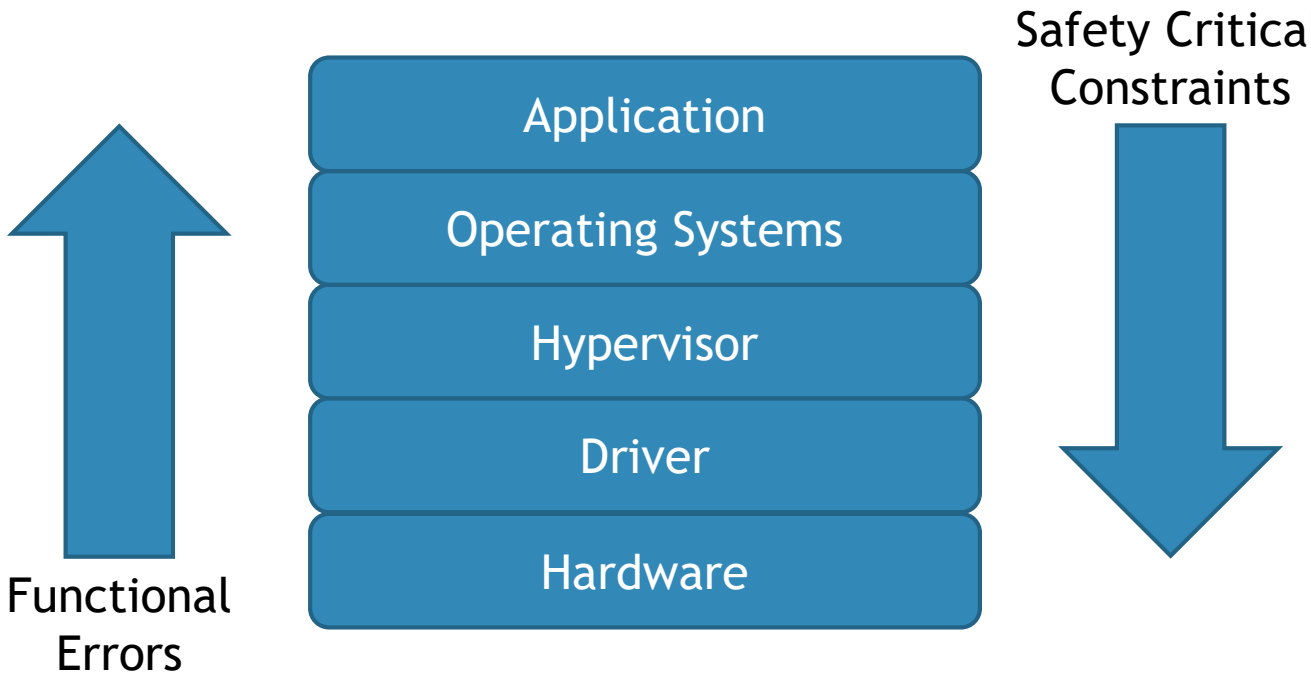

ANNUAL GLOBAL ROAD CRASH STATISTICS
RIP
Nearly
1.3 MILLION
people die in road crashes each year, with an average of
3,287
deaths per day.
An additional
20-50 MILLION
are injured or disabled.
More than HALF
of all road traffic deaths occur among people ages
15-44
Road crashes cost
$518 BILLION
per year and are predicted to become the
5TH LEADING
overall cause of death by 2030.
Around
1,000
people under the age of 25
die on the roads each day.
For ages 15-29,
road crashes are the LEADING cause of death and for ages
2-14,
the SECOND LEADING cause of death.
Z&D
Zinda & Davis
Source: http://asirt.org/Initiatives/Informing-Road-Users/Road-Safety-Facts/Road-Crash-Statistics

COREAVI

Safety Principals Create Constraint

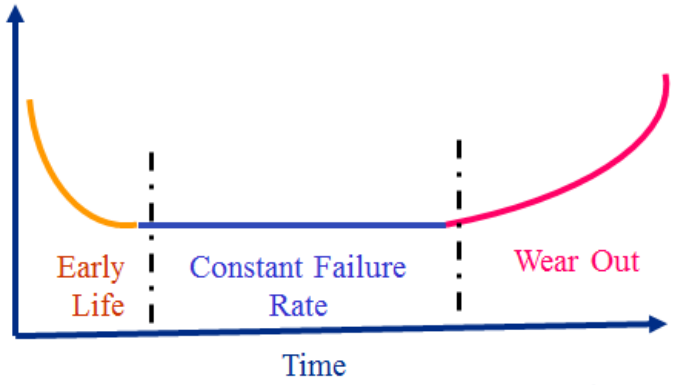
- Deterministic
- Bounded (in space and time)
- Non blocking code (no semaphores)
- Interrupts challenge time boundaries
- Error/failure detecting
- Defining what is an error or failure

Safety Critical Stacking



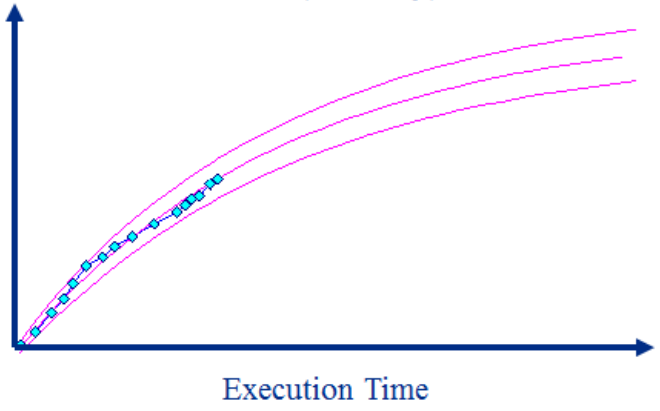
COREAVI

Hardware and Software Reliability Relationship



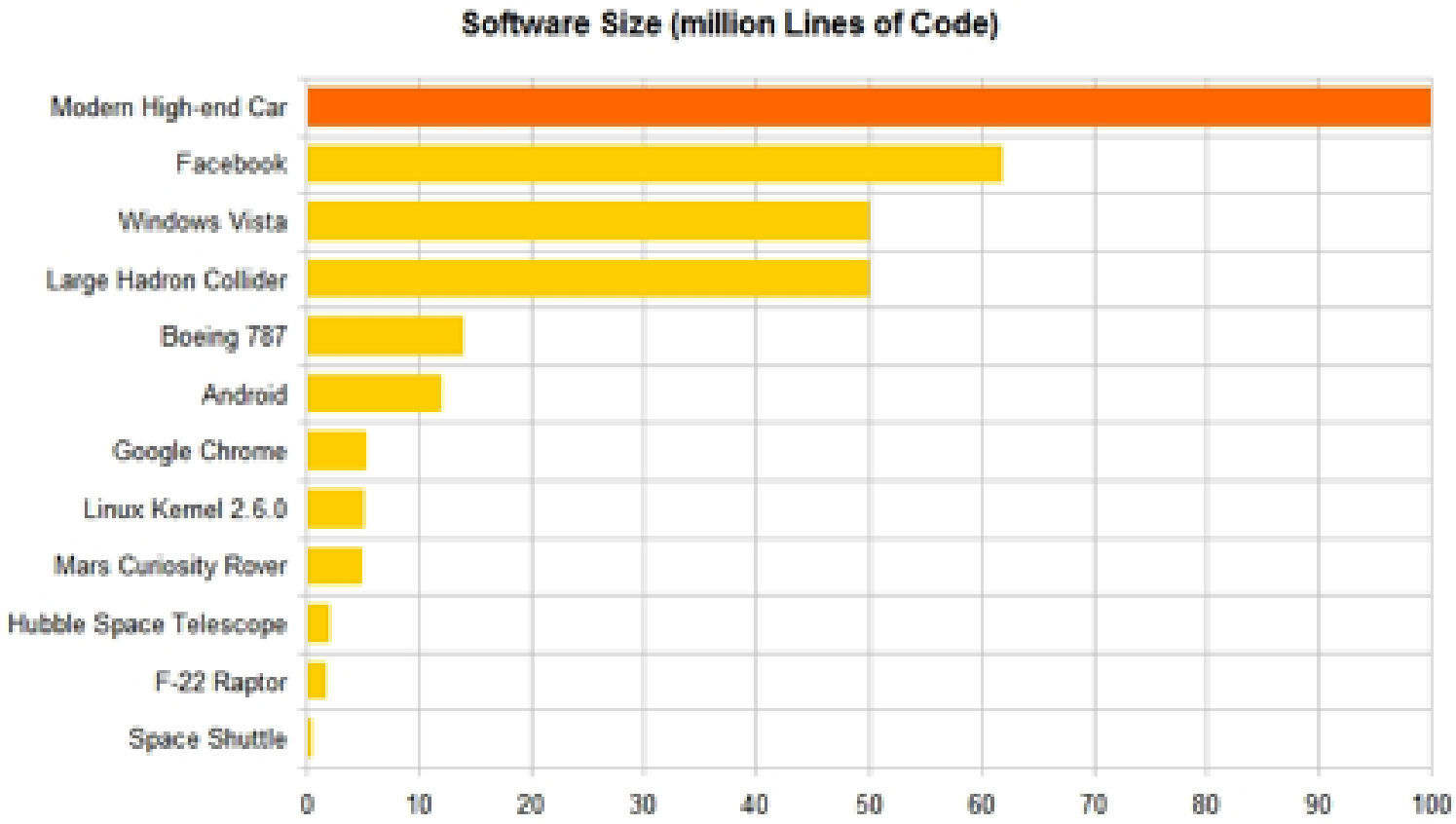
HW Reliability
Three Phases
1. Early Life, Debugging
2. Constant Failure Rate
3. Wear Out

SW Reliability
Reliability Growth
(Stability) over time



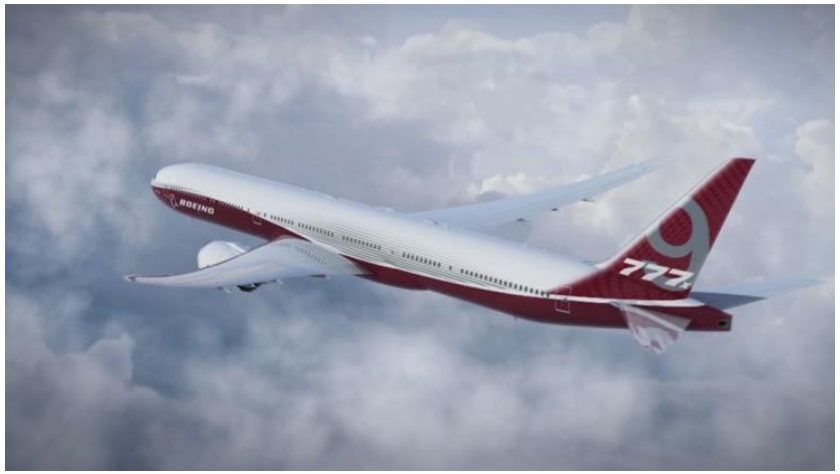
COREAVI

Relative Software Complexity will Increase



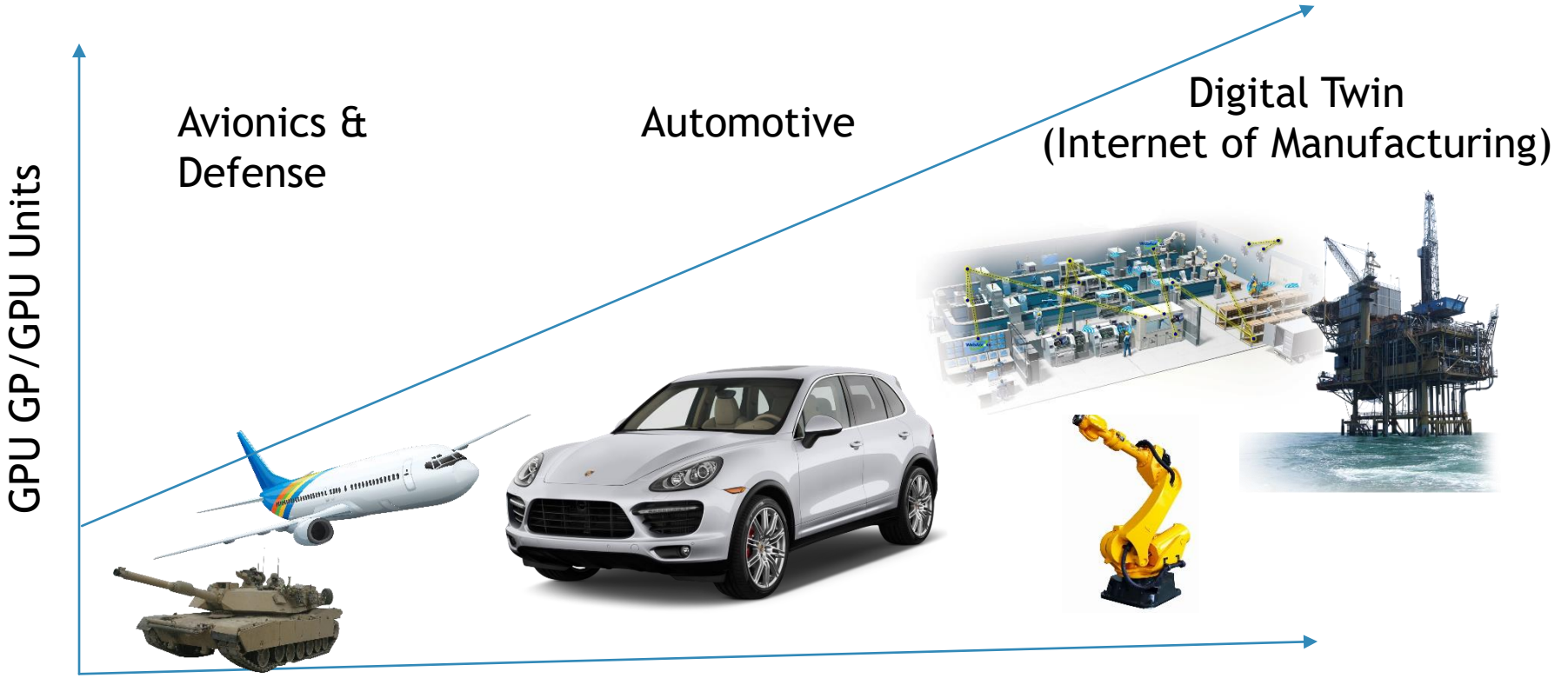
COREAVI

Safety Applications



COREAVI

Safety Critical Graphics and Compute



Functional Safety SIL IEC 61508

ISO 26262

RTCA DO-178C
EUROCAE ED-12C
Avionics

FEDERAL AVIATION ADMINISTRATION

IEC 60880

EN 50128

COREAVI

Trends in the Automotive Digital Cockpit

Addressing the safety requirements in Digital Cockpit designs

- ASIL B for safety elements of HMIs
- Digital Instrument Cluster (telltales)
- Heads Up Display
- Blind Spot Monitor
- Digital Side-View Displays (mirror replacement)
- Lane Departure Warning
- On the horizon - ASIL B (or greater) for ADAS/Autonomous workloads using graphics as an accelerator

Consolidation and mixed ASIL support is a must have.

** Use Authorized by Arm Holdings, 2018*

COREAVI

Safety Technology Drivers

- Increased demand for functionality and capability, with safety, requires added attention and investment
- Safety certifiable is a becoming a broader need, evolving from what was previously a limited market requirement
- Cost and reusability are determining factors and subject to continued competitive pressure
- Disruption in technologies and approaches (ARM replacing PowerPC, Vulkan replacing OpenGL, standardized hardware requirements, increased certification)

The Future of GPU Deployment

- GPU support embedded in low power, performance oriented SOCs provide an alternative to discrete GPU systems
- The division of labor between CPUs, GPUs and dedicated compute engines within SOCs will increase overall system performance
- Khronos Group has formed a working group for Vulkan SC activities and an initial specification is under review
- Safety critical applications evolve to take advantage of Vulkan SC graphics and compute performance

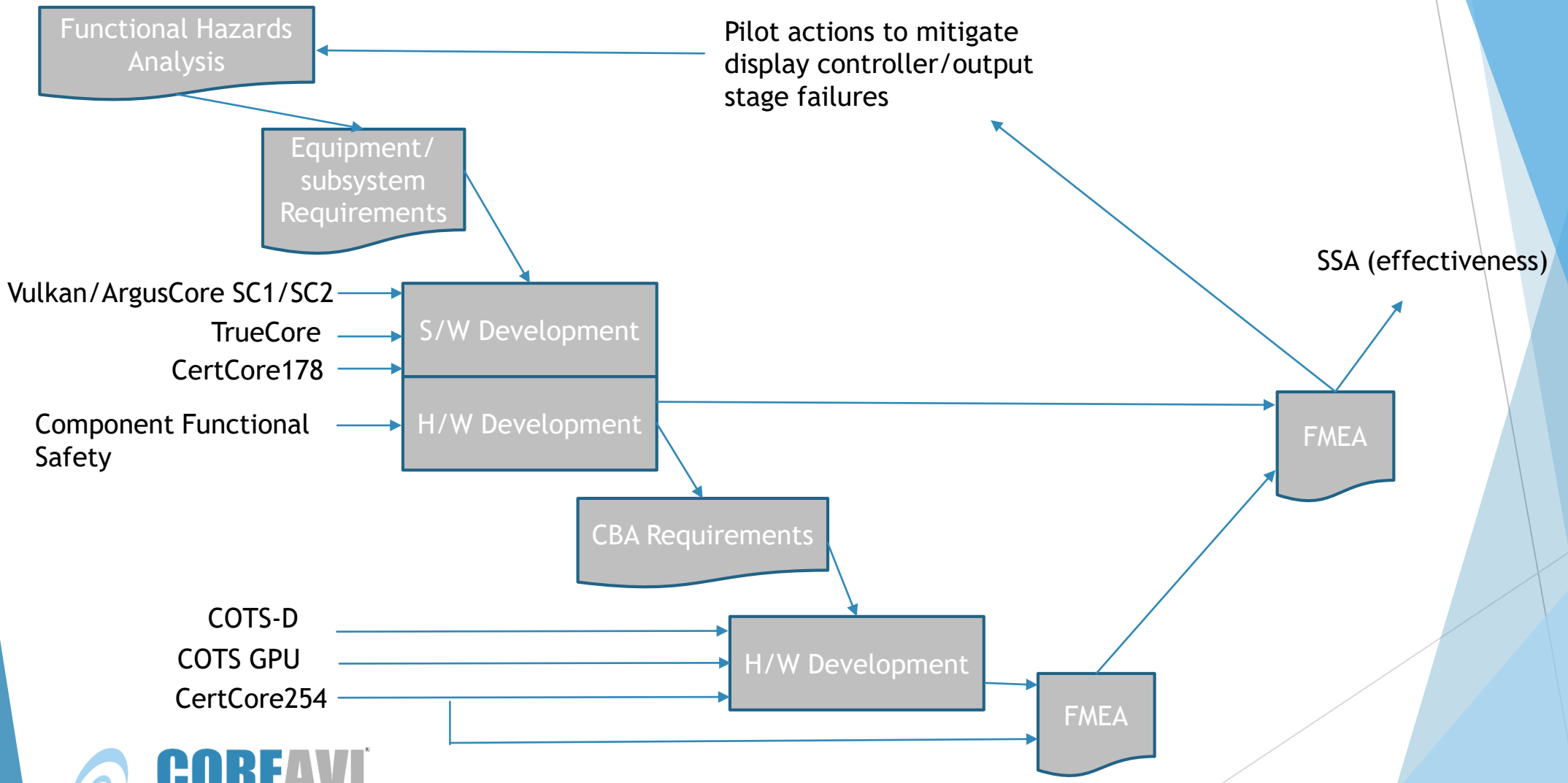
What Vulkan SC Offers

- First safety critical compute open standard
- Allows development of a multi-use platform of safety certifiable applications through graphics and computer hardware abstraction
- Improves GPU performance on a per watt basis and reduces impact on the CPU, thereby lowering system cost for similar performance
- Supports graphics and compute in a single interface, increasing functionality and flexibility from a given hardware platform
- Gives access to more advanced graphics functions than either OpenGL SC 1.0 or 2.0 such as geometry shaders and multiple render targets

Machine Learning Trends

- Today, neural network algorithms primarily are deployed to classify big data to identify trends and to target advertising
- Today, embedded system decision making is based on fixed, relatively simple algorithms, created by human programmers from historical experience
- Complex autonomous machines will increasingly be managed by neural network algorithms that employ independent situational (machine) learning
- Future embedded systems will make decisions based on learning algorithms that will change without human reprogramming
- GP-GPU computing is a powerful solution for compute intensive applications, initially in the cloud (big data) but evolving into embedded systems
- Safety critical compute and Vulkan SC will play a role in the evolution of neural network based machine learning software

System Safety Assessment



Safe, Very Safe, and Safe Enough

- First and last development priority
- Management and communication of risk is imperative, high reliability organizations begin and end with safety
- Safety critical demands “fit for purpose” consideration at the system level
- Standards and certification practices make safety more straight forward and demonstrable
- Goals for safety critical implementations:
  - Efficient
  - Effective
  - Risk Reducing

Silicon Provider Role

- Formal functional safety programs, the foundation of safety
- Consideration of long term reliability at the design and at the process level
- Integrate functional BIT and error detection logic such as ECC in memory
- Institute FMEA process across design and manufacturing
- Recognize that FIT rate impacts real life safety, it is not a theoretical exercise
- Recognize that the majority of high reliability system experience (data) is at 28 - 45 nm nodes

We always overestimate the change that will occur in the next two years and underestimate the change that will occur in the next ten

Bill Gates

COREAVI

COREAVI®

~ When It's Critical ~

Thank You

www.coreavi.com