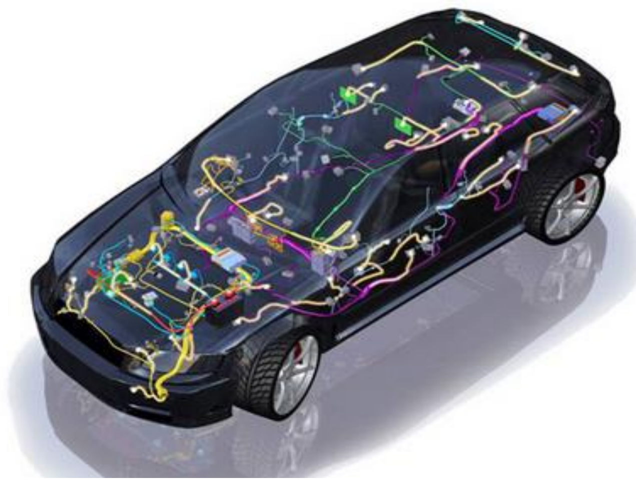
DfR Solutions
RELIABILITY DESIGNED & DELIVERED

# 2018 DESIGN for RELIABILITY CONFERENCE

Real-World Applications of Physics of Failure Solving Today's Technology Challenges

# Applying Reliability Physics Analysis to ISO-26262 Functional Safety Hardware Reliability Assessments

ISO 26262
Road Vehicles - Fuctional Safety



Keith Hodgson – E/E Reliability Lead Ford Motor Co.
James McLeish – DfR Solutions

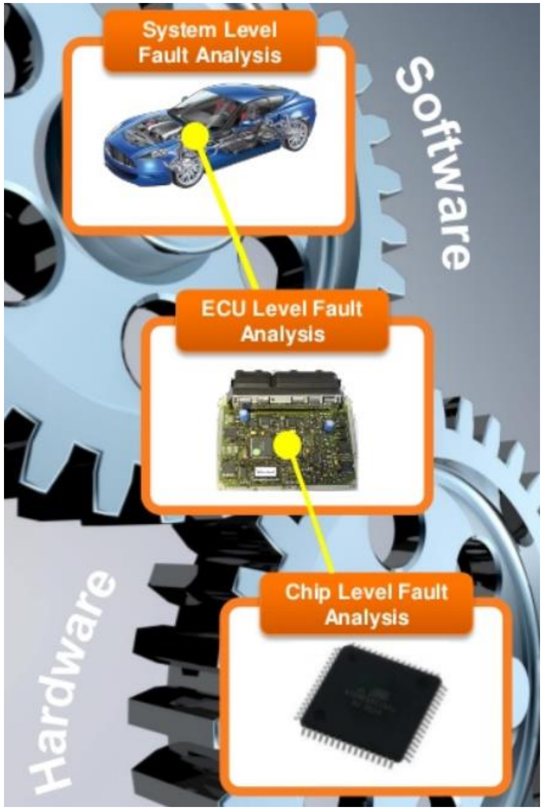
# Presenter's Bios

- **Keith M. Hodgson has been at Ford Motor since 1990, started at the Electronics Division (now Visteon).**
  - He is a Senior Reliability/Test Engineer supporting Ford Design and Release engineers around the world.
  - He is Ford's Subject Matter Expert (SME) for Electrical/Electronic Reliability and Test methods and is the owner of Ford's Corporate Engineering Test Procedure, CETP 00.00 E 412, E/E Component Environmental Compatibility Tests.
  - He has been a champion for the implementation of Physics of Failure, methods at Ford since the late 1990s and is leading the effort to incorporate PoF methods in all new designs with 1st & 2nd tiers E/E suppliers worldwide.
  - He previously worked at the Buick Motor Division of General Motors from 1983 to 1990 and was part of the team that put the Buick LaSabre on the top 10 list for vehicle quality.
  - He's been actively involved in test engineering since 1978, sits on the USCAR E/E committee, is the Chairman of the SAE E/E Systems Reliability Standards & Sponsor of the SAE J3168 Reliability Physics Analysis Std. now in development.
- **James (Jim) McLeish heads the Midwest regional office of DfR Solutions**
  - He has 40 years of automotive, military and industrial E/E design engineering and product assurance experience, starting his career as an automotive electronics design product engineer on the team that invented the first Microprocessor based Engine Controller at Chrysler in the 1970's.
  - He has previously worked at Chrysler, General Motors & GM Defense in vehicle E/E systems engineering, design, development, product, validation, reliability and quality assurance.
  - He holds an MSEE degree and 3 patents in embedded control systems, is an author/co-author of 3 GM E/E Validation Test/Reliability-Durability demonstration standards, SAE J-1211 and is a co-leader on the new SAE J3168 RPA Std.
  - He is credited with the introduction of Reliability Physics methods to GM while serving as the E/E Reliability Manager and QRD Technical Expert.
  - He is a senior member and Regional Director of the ASQ Reliability & Risk Division, and a core member of the SAE Automotive Reliability Standards and the Reliability Lead on the SAE ISO-26262 Functional Safety Committee.

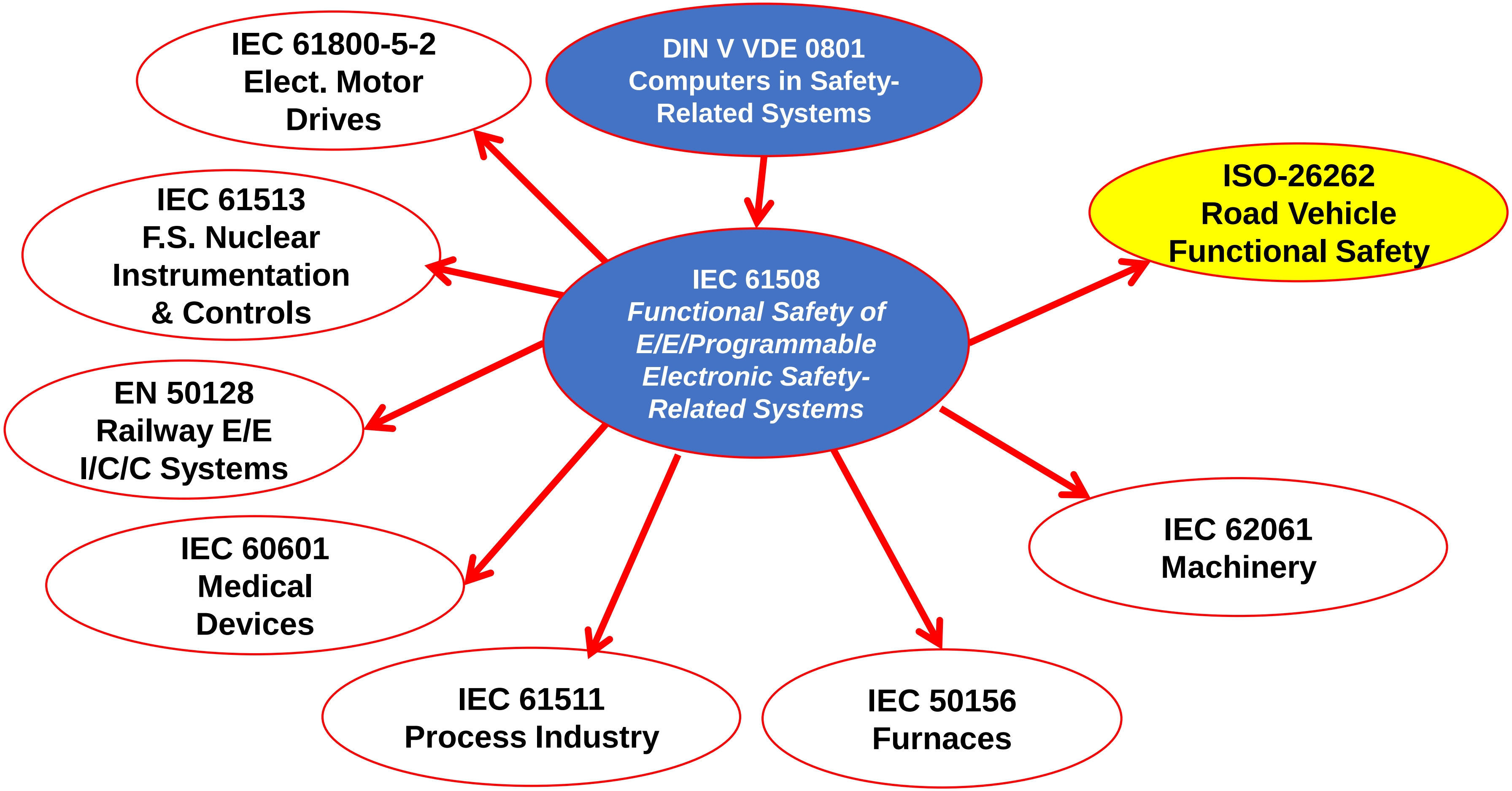
  

# ISO 26262 Road Vehicles - Functional Safety

- ISO 26262 is E.U. standard for safety related EE systems in passenger cars. (Expanding to include Trucks and Motorcycles in 2018 )
- 26262 addresses possible hazards caused by malfunctions within & between E/E safety-related/critical systems.
- Evolved from IEC 61508 "Functional Safety of E/E & Programmable Electronic Systems“ & led to the creation of other FS Standards.

# Migration of Functional Safety Standards



# ISO 26262-2011 has 10 parts, the 2018 Revision will have 12 Parts

2011/2012

| | | Pages | Reg. $ | Member $ |
|---|---|---|---|---|
| 1. | Vocabulary | 23 | $138.00 | $110.40 |
| 2. | Mgmt. of Funct. safety | 26 | $138.00 | $110.40 |
| 3. | Concept Phase | 25 | $138.00 | $110.40 |
| 4. | Product System-level | 26 | $185.00 | $148.00 |
| 5. | Product Development HW (Includes HW Reliability) | 76 | $209.00 | $167.20 |
| 6. | Product Development SW | 40 | $185.00 | $148.00 |
| 7. | Production & Operations | 11 | $ 68.00 | $ 54.40 |
| 8. | Supporting Processes | 48 | $185.00 | $148.00 |
| 9. | ASIL & Security Analysis | 16 | $103.00 | $ 82.40 |
| 10. | Guideline Examples 72 | $232.00 | $186.60 | 85 |
| 11. | Semiconductor | | ----N/A---- | ----N/A---- |
| 12. | Motorcycle | | ----N/A---- | ----N/A---- |
| | TOTAL: | 363 | $1,581.00 | $1,265.80 |
| | Avg. Price per page | | $4.36 | $3.49 |
| | Package Price: | | $1049.00 | $839.20 |

## ISO 26262 Attributes

**Large**

**Complex**

**Inter-Related**

**Expensive**

# Functional Safety – An Evolution in Safety Engineering

- **Evolving from a focus on accident prevention & "add-on" protection to "Inherent Safety"**
  - Ensuring that systems/equipment always operate correctly in response to their inputs.
  - Achieved by "Designing Out" susceptibilities to potential hazards & failure risks for both:
    - Random Failures - Physical failures due usage, environmental & wearout conditions.
    - Systematic Failures - due to human error in design, manufacture & operation


- **The standards for functional safety are relatively new**
  - The Legalize Language used seems to be ambiguous and difficult to interpret.
  - Users have found it challenging to interpret and to apply these standards.

- **Weakly Recommends Applying "Lessons Learned" & Producing "Robust Design"**
  (Each mentioned only once, in one sentence each.
  - Intense focus on complex probabilistic mathematics to predict random failures risks.

- **<u>PURPOSELY NON-PRESCRIPTION</u>**
  - No-Little Guidance on how to Achieve Reliability & Safety.
  - Intent is that the intense analysis will foster the creation of inventive solutions.

- **Significantly more difficult to manage/predict the risk of systematic failures, including the safe management of likely design & operator errors.**

## ISO-26262-2011 Part 5 (Hardware) Requires Safety Risk Assessments & Defines Max Probabilities for the Violation of Each Safety Element Goal

### "Probabilistic Metric for (random) Hardware Failures" (PMHF)

- Initially appeared that PMHF was a max allowable failure rate for use in Safety Violation Risk Analysis based on Automotive Safety Integrity Levels ((ASIL) criticality scale).

| ASIL | FAILURE RATES λ | Random hardware failure target values | 1 / λ = MTBF |
|---|---|---|---|
| D | 0.00000001 Violations/Hr. | $< 10^{-8}$ $h^{-1}$ | 100,000,000 Fleet Hrs. (10 FIT) |
| C | 0.00000010 Violations/Hr. | $< 10^{-7}$ $h^{-1}$ | 10,000,000 Fleet Hrs.(100 FIT) |
| B | 0.00000010 Violations/Hr. | $< 10^{-7}$ $h^{-1}$ | 10,000,000 Fleet Hrs.(100 FIT) |
| NOTE The quantitative target values described in this table can be tailored as specified in 4.1 to fit specific uses of the item (e.g. if the item is able to violate the safety goal for durations longer than the typical use of a passenger car). | | | |

*FIT (Failure in Time) (Failures/Billion Fleet Operating hours ($10^{-9}$)V*

- 8.4.3 This requirement applies to ASIL (B), C, and D of the safety goal.

  The estimated failure rates for hardware parts used in the analyses shall be determined by:

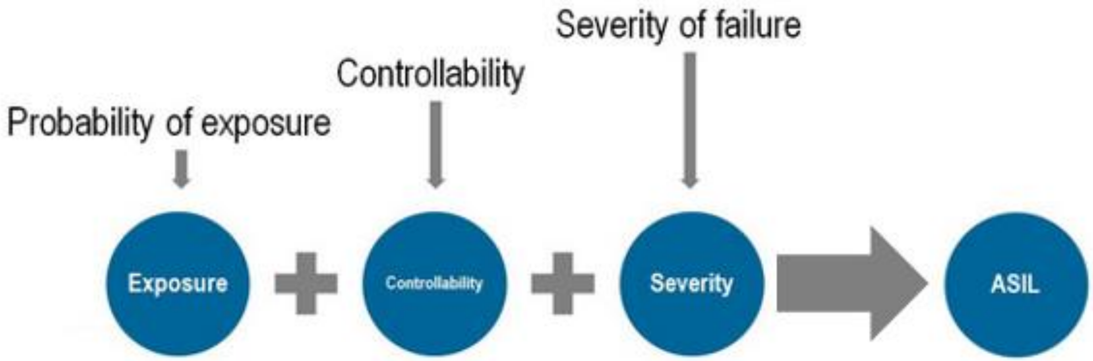
  a) Using ***(ACTUARIAL)*** **hardware part failure rates data from a recognized industry source.** Examples:
  **(IEC/TR 62380 (Telecom), IEC 61709 Generic E/E components), EN 50129:2003-C, (Rail Equip), IEC 62061:2005 (machinery), MIL HDBK 217F-2, & RIAC: 217 Plus, NPRD 95 – Nonelect. Parts Reliability Data, MIL HDBK 338 (EE Reliability Design HDBK). RIAC-FMD (Failure Mode Distributions), UTE C80-811 (Fides -French MIL), SN 29500 (Siemen German Industrial)**
  *NOTE 1 The failure rate values given in these databases are generally considered to be pessimistic.)*

  b) Or using **statistics from field returns or tests.**

  c) Or using **expert judgement based on an engineering approach** based on quantitative & qualitative arguments. Criteria for expert judgment can include field experience, testing, reliability analysis & novelty of design.

# Automotive Safety Integrity Level (ASIL) (Critically Determination)

- The ASIL Criticality Classification of every System & "Hardware Elements (i.e. Circuit Branches) in a system is determined at the start of program by a 26262 process called: **"Hazard Analysis and Risk Assessment" (HARA),** that evaluates:
  - Severity (S) – measure extent of potential harm/loss caused by a failure (4 categories)
  - Exposure (E) – probability of exposure (5 Categories)
  - Controllability (C) – of the potential hazard (4 Categories)

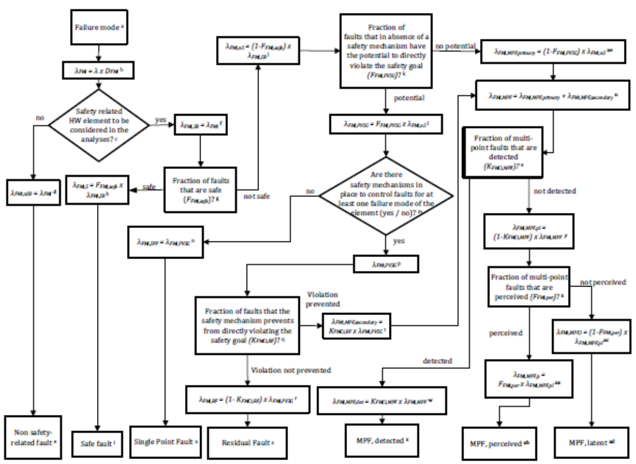



- **A risk table uses the S, E & C ratings to determine the ASIL.**
  - 4 ASIL Ratings (A lowest – D highest, plus NON ASIL QM (Apply Normal Quality Methods).
  - ASIL ratings are used throughout 26262 to specify various level of requirements
    - Also Ref: SAE J2980 "Considerations for ISO 26262 ASIL Hazard Classification"

# PMHF Calculations *(from 3 of 28 Pages of PMHF Calculation Requirements in 2018 part 10)*

**Flow diagram for fault classification and calculation of corresponding failure rates**



Where

| | |
|---|---|
| $M_{PMHF}$ | is the PMHF value determined using ISO 26262-5:2018, 9.4.2.2 |
| $\lambda_{SPF}$ | is the single point failure rate |
| $\lambda_{RF}$ | is the residual failure rate |
| $\lambda_{IF,DPF}$ | is the dual point failure rate for IF |
| $\lambda_{IF,DPF,detected}$ | is the IF's detected and notified dual point failure rate |
| $\lambda_{IF,DPF,latent}$ | is the IF's latent dual point failure rate (mitigated but not notified) |
| $\lambda_{SM1,DPF}$ | is the SM1's dual point failure rate |
| $\lambda_{SM1,DPF,detected}$ | is the SM1's detected and notified dual point failure rate |
| $\lambda_{SM1,DPF,latent}$ | is the SM1's latent dual point failure rate |
| $T_{lifetime}$ | is the vehicle lifetime |
| $T_{service}$ | is the expected time to repair after notification provided to driver |

$$
\begin{aligned}
M_{PMHF} = \lambda_{SPF} + \lambda_{RF} & \\
+ 0{,}5 * \lambda_{SM1,DPF,latent} * \lambda_{IF,DPF} * T_{lifetime} & \quad \text{Pattern 1} \\
+ \lambda_{SM1,DPF,detected} * \lambda_{IF,DPF} * T_{service} & \quad \text{Pattern 2} \\
+ 0{,}5 * \lambda_{IF,DPF,latent} * \lambda_{SM1,DPF} * T_{lifetime} & \quad \text{Pattern 3} \\
+ \lambda_{IF,DPF,detected} * \lambda_{SM1,DPF} * T_{service} & \quad \text{Pattern 4}
\end{aligned}
$$

$\lambda_{IF,DPF} = \lambda_{IF,DPF,primary} + \lambda_{IF,DPF,secondary}$

$\lambda_{IF,DPF,primary} = (1-F_{IF,safe})*(1-F_{IF,PVSG})*\lambda_{IF}$

$\lambda_{IF,DPF,secondary} = (1-F_{IF,safe})*F_{IF,PVSG}*K_{FMC,SM1,RF}*\lambda_{IF}$

$\lambda_{IF,DPF,detected} = \lambda_{IF,DPF,detected,primary} + \lambda_{IF,DPF,detected,secondary}$

$\lambda_{IF,DPF,detected,primary} = \lambda_{IF,DPF,primary} * K_{FMC1,SM1,MPF} = (1-F_{IF,safe})*(1-F_{IF,PVSG}) * K_{FMC1,SM1,MPF} * \lambda_{IF}$

$\lambda_{IF,DPF,detected,secondary} = \lambda_{IF,DPF,secondary} * K_{FMC2,SM1,MPF} = (1-F_{IF,safe})*F_{IF,PVSG}*K_{FMC,SM1,RF}*K_{FMC2,SM1,MPF}*\lambda_{IF}$

$\lambda_{IF,DPF,latent} = \lambda_{IF,DPF,latent,primary} + \lambda_{IF,DPF,latent,secondary}$

$\lambda_{IF,DPF,latent,primary} = \lambda_{IF,DPF,primary} * (1-K_{FMC1,SM1,MPF}) = (1-F_{IF,safe})*(1-F_{IF,PVSG})*(1-K_{FMC1,SM1,MPF})*\lambda_{IF}$

$\lambda_{IF,DPF,latent,secondary} = \lambda_{IF,DPF,secondary} * (1-K_{FMC2,SM1,MPF}) = (1-F_{IF,safe})*F_{IF,PVSG}*K_{FMC,SM1,RF}*(1-K_{FMC2,SM1,MPF})*\lambda_{IF}$

$\lambda_{SM1,DPF} = \lambda_{SM1,DPF,primary} + \lambda_{SM1,DPF,secondary}$

$\lambda_{SM1,DPF,primary} = (1-F_{SM1,safe})*(1-F_{SM1,PVSG})*\lambda_{SM1}$

$\lambda_{SM1,DPF,secondary} = (1-F_{SM1,safe})*F_{SM1,PVSG}*K_{FMC,SM2,RF}*\lambda_{SM1}$

$\lambda_{SM1,DPF,detected} = \lambda_{SM1,DPF,detected,primary} + \lambda_{SM1,DPF,detected,secondary}$

$\lambda_{SM1,DPF,detected,primary} = \lambda_{SM1,DPF,primary} * K_{FMC1,SM2,MPF} = (1-F_{SM1,safe})*(1-F_{SM1,PVSG}) * K_{FMC1,SM2,MPF} * \lambda_{SM1}$

$\lambda_{SM1,DPF,detected,secondary} = \lambda_{SM1,DPF,secondary} * K_{FMC2,SM2,MPF} = (1-F_{SM1,safe})*F_{SM1,PVSG}*K_{FMC,SM2,RF}*K_{FMC2,SM2,MPF}*\lambda_{SM1}$

$\lambda_{SM1,DPF,latent} = \lambda_{SM1,DPF,latent,primary} + \lambda_{SM1,DPF,latent,secondary}$

$\lambda_{SM1,DPF,latent,primary} = \lambda_{SM1,DPF,primary} * (1-K_{FMC1,SM2,MPF}) = (1-F_{SM1,safe})*(1-F_{SM1,PVSG})*(1-K_{FMC1,SM2,MPF})*\lambda_{SM1}$

$\lambda_{SM1,DPF,latent,secondary} = \lambda_{SM1,DPF,secondary} * (1-K_{FMC2,SM2,MPF}) = (1-F_{SM1,safe})*F_{SM1,PVSG}*K_{FMC,SM1,RF}*(1-K_{FMC2,SM2,MPF})*\lambda_{SM1}$

Where

| | |
|---|---|
| $\lambda_{IF}$ | is the IF's failure rate |
| $\lambda_{SM1}$ | is the SM1's failure rate |
| $F_{IF,safe}$ | is the ratio of safe faults of the IF |
| $F_{SM1,safe}$ | is the ratio of safe faults of SM1 |
| $F_{IF,PVSG}$ | is the ratio of faults of the IF that have the potential to directly violate a safety goal in absence of a safety mechanism |
| $F_{SM1,PVSG}$ | is the ratio of faults of SM1 that have the potential to directly violate a safety goal in absence of a safety mechanism |

**Table 2 — Patterns of dual point failure in the example architecture**

| | First fault:SM1 ➔ Second fault: IF | First fault: IF ➔ Second fault: SM1 |
|---|---|---|
| Cannot notify the driver | Pattern 1<br><br>A fault in SM1 is mitigated by SM2 but not notified. The exposure duration of the fault is taken as the vehicle lifetime which is the worst case exposure duration.<br><br>Or<br><br>A fault in SM1 is not mitigated by SM2. The exposure duration of the fault is taken as the vehicle lifetime which is the worst case exposure duration. | Pattern 3<br><br>A fault in IF is mitigated by SM1 but not notified. The exposure duration of the fault is taken as the vehicle lifetime which is the worst case exposure duration. |
| Can notify the driver | Pattern 2<br><br>A fault in SM1 is mitigated and notified by SM2. The exposure duration of the fault is taken as the expected time required for the driver to take the vehicle in for repair. | Pattern 4<br><br>A fault in IF is mitigated and notified by SM1. The exposure duration of the fault is taken as the expected time required for the driver to take the vehicle in for repair. |

Mindset is that such extensive calculations are needed to justify the cost of "Safety Mechanism" to auto company management

## ISO-26262-2018 Part 10 "Guidelines" PMHF Definition
## "Average Probability (of Safety Goal Violation) per Hour"

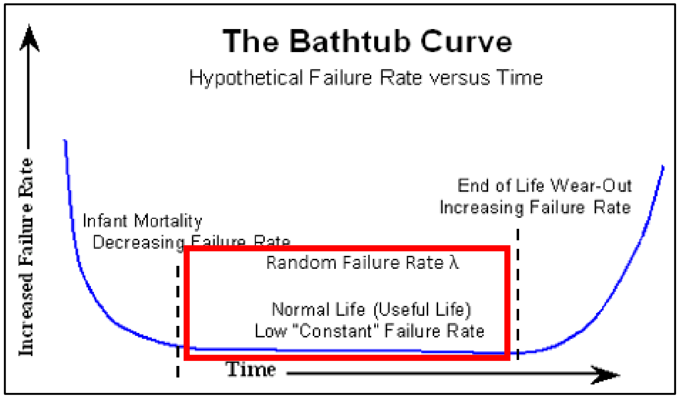
- *"While Reliability analysis provides the failure rate for individual components or parts*
- *Functional safety instead considers the effect of:*
  - ***Fault detection, control and notification functions provided by safety mechanisms.***
  - ***Therefore, even if the "Events/Hour" units are the same as in reliability analysis, the meaning is not the same."***

- The PMHF calculation determines if the risk of safety goal violation, due to random hardware failure of the item is sufficiently low, relative to the Severity Level (ASIL).
  - PMHF does not correlate to how often random hardware failures/faults occur.
  - Even if the failure rate of a hardware element is high, the PMHF may be low due to good hardware architectural design that includes adequate safety mechanisms.
  - If the sum of the failure risk is larger than the max allowable PMHF values in the Part 5 PMHF Table 6, then the system is not acceptable and has to be redesign to either improve reliability (i.e. reduce failure risks) or add addition levels of safety mechanisms.

- **However PMHF is primarily based in Actuarial Reliability Prediction handbooks methods that by definition do not include wear out data.**

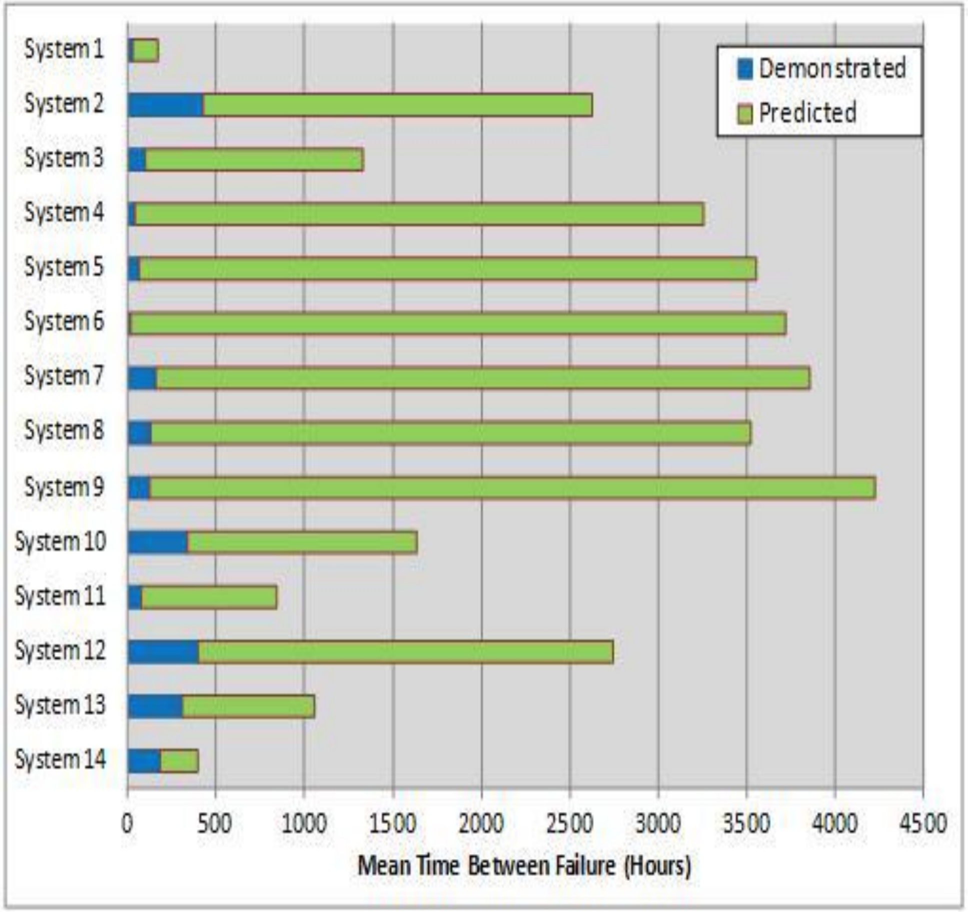
# Shortcoming of Actuarial, MTBF Reliability Prediction Methods




- **Limited to constant failure rates (i.e. random failure) ignores infant mortality and wearout related failures.**
- **Industry wide average failure rates are not vendor, device or event specific, ignores physics & mechanics of failure.**
- **At least 78% of electronic failures not modeled by 217***
  ** "A Comprehensive Reliability Assessment Tool for Electronic Systems", RAMS 2001*
  - **Design errors, assembly issues, solder and wiring failures, PCB insulation breakdown and via failures, software errors . . . etc.**
- **Over emphasis on the Arrhenius model and steady state temperature as the primary factor in electronic component failure.**
- **Keeping failure rate data up to date is difficult, costly & underfunded**
  - **Vast number of component types/suppliers, rapid technology advancement & QRD growth**
- **E/E Tech Rapidly Evolves.**
  - **New components and materials will have different failure susceptibilities than past generations, so the use of even recent F.R. data may not be reflect real work performance.**

# Actuarial Reliability Prediction vs Actual Reliability

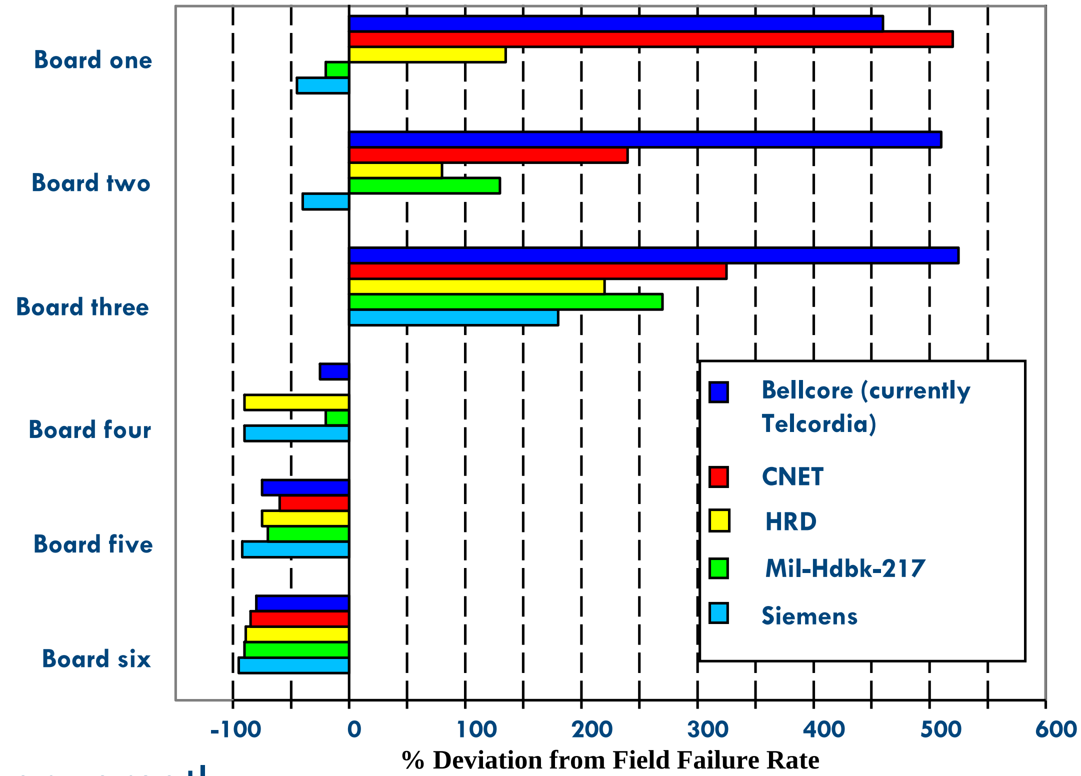
- **Accuracy study found that even when reliability data is based on the same E/E tech as actual products.**
  - Actuarial predictions significantly over estimate demonstrated reliability.
  - *Because actuarial data can* not keep up with modern continuous improvement efforts of the E/E components.
    - *Source - RAMS 2013: "Reliability Predictions – Continued Reliance on a Misleading Approach" by Christopher Jais, et al, US Army Materiel Systems Analysis Activity*




  www.DfRsolutions.com DfR Solutions RELIABILITY DESIGNED & DELIVERED

# Accuracy Issues of Empirical Actuarial Reliability Prediction Handbooks

- Loughborough a Senior fellow at NASA found deviations greater than 500%.
- How can data and processes this diverse, be trusted for use in Safety Planning of Autonomous Vehicles




- Results from different handbook can vary greatly
- Failure rate predictions can be off by as much as 10,000X from actual field failure rates.

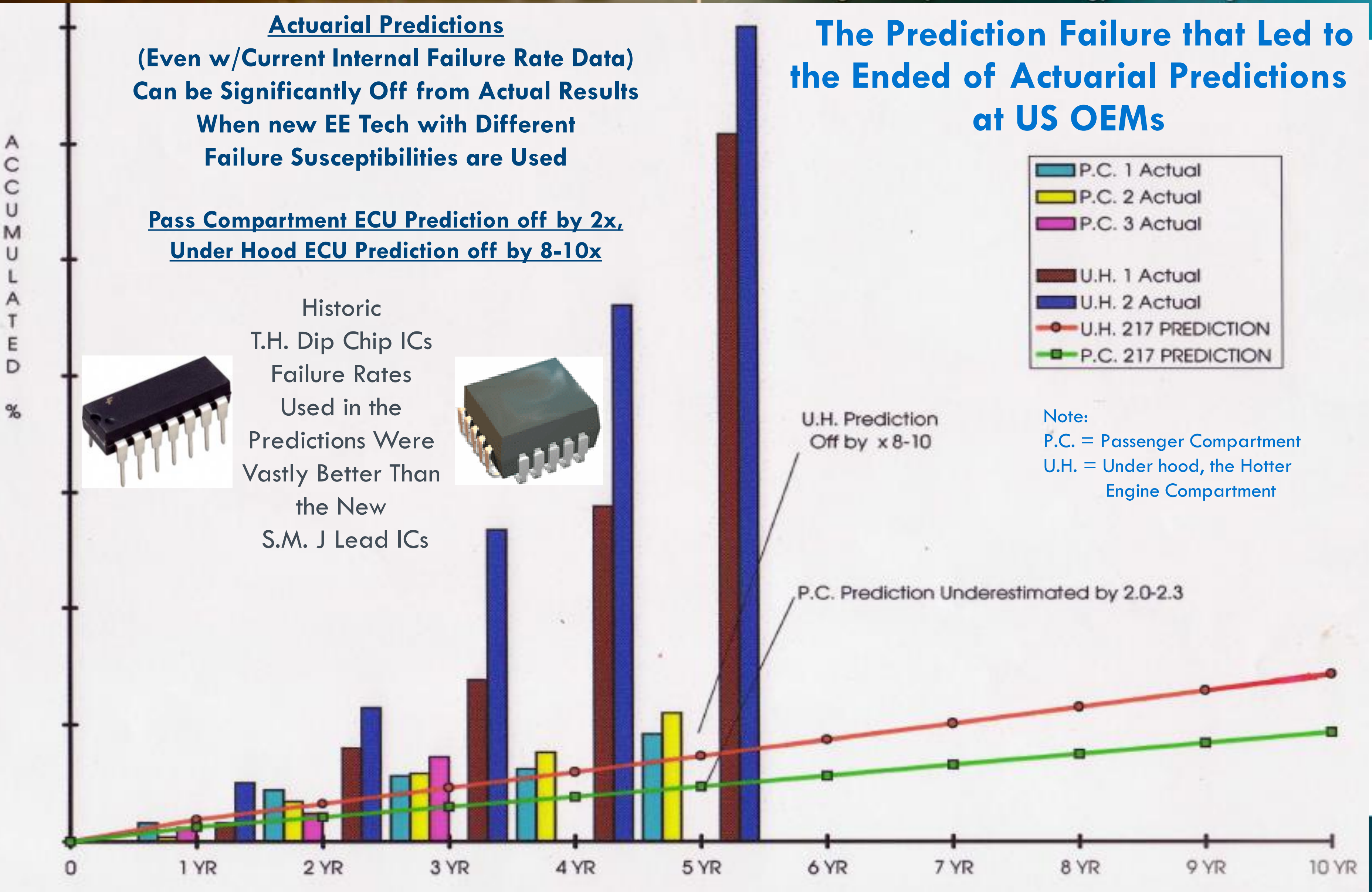
# The Prediction Failure that Led to the Ended of Actuarial Predictions at US OEMs

**Actuarial Predictions**

**(Even w/Current Internal Failure Rate Data) Can be Significantly Off from Actual Results When new EE Tech with Different Failure Susceptibilities are Used**

**Pass Compartment ECU Prediction off by 2x, Under Hood ECU Prediction off by 8-10x**

Historic T.H. Dip Chip ICs Failure Rates Used in the Predictions Were Vastly Better Than the New S.M. J Lead ICs




Note:
P.C. = Passenger Compartment
U.H. = Under hood, the Hotter Engine Compartment

## 26262 Excessively Focuses on Electronics & Ignores Systems & Mech. Interfaces

- **Infamous Safety Issues 26262 Would Not Identify:**
  - **1986 Audi Start Up Sudden Accelerations.**
    - Proven Root Cause – Drive Accidently Depresses Gas Pedal Instead of Brake Pedal
    - Fix: <u>BTSI (Brake Transmission Shift Interlock)</u> A system that prevents driver from start the vehicle & shifting out of park until the brake pedal is fully depressed.
  - **Mid-2000's Toyota Unintended Acceleration (a motivator for creating ISO-26262).**
    - Intense Initial Focus on Toyota's Electronic "Throttle by Wire" & "Cruise Control" Electronics
    - Proven Root Cause: Floor Mat-Gas Pedal jamb / Sometime a mechanically sticky gas pedal linkage.
    - Fix: Reduce size of gas pedal, Floor Mat position snaps & <u>"Brake Overrides Gas"</u> logic
  - **2014 Takata Airbag Igniter.**
    - Proven Root Cause: Use of cheap, unstable ammonium nitrate propellent that become more energetic as it ages, resulted in fragmentation grenade behavior that killed or injured scores of people.
    - Fix: Replaced with igniters that use a stable propellant.
  - **2014 GM Ignitions Switch Engine Self Shut-Off.**
    - Proven Root Cause: Ign. Sw. mechanical detent was insufficient to prevent accidental rotation out of the on state resulting in a vehicle shutdown and lost control .
    - Fix: Replace with a Correctly Configured Ignition Switch.

# ISO-26262-2018 Part 5 (Hardware) will Recognize Physics of Failure durability simulation as valid for use in PMHF safety risk assessments

**8.4.3** This requirement applies to ASIL (B), C, and D of the safety goal. The estimated failure rates for hardware parts used in the analyses shall be determined:

c) using expert judgement founded on an engineering approach based on quantitative and qualitative arguments. Expert judgement shall be exercised in accordance with structured criteria as a basis for this judgement. These criteria shall be set before the estimation of failure rates is made.

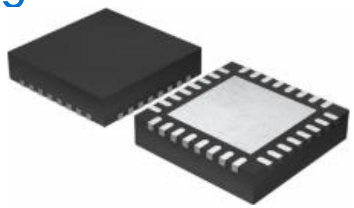
NOTE 6 The criteria for expert judgment can include a combination of heuristic information supported by a combination of field data, testing, reliability analysis and physics-of-failure based simulation approaches while considering the novelty of the design.

NOTE 7 Informative references from international reliability expert bodies can be used: SAE J1211 "Robustness Validation" – Analysis, Modelling and Simulation provides physics-of-failure (PoF) based failure mechanism models, JEDEC-JESD89, JEDEC-JESD91, JEDEC-JESD94, JEDEC-JEP143, JEDEC-JESD148.

# Achieving Durability-Reliability for the Advanced Electronics Tech for Autonomous Vehicles Require will be the Next Challenge

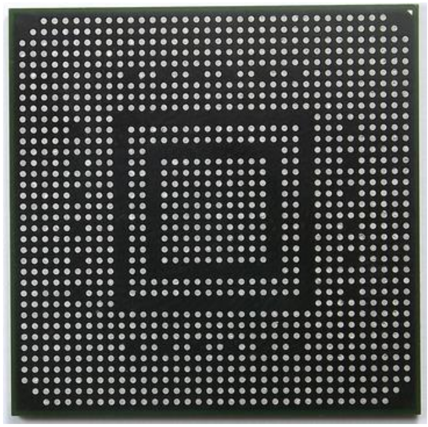
## Leading Durability-Reliability Challenges in Advanced Automotive Electronics

1) Tiny/Fragile Flat No Lead / Near Chip Scale Integrated Circuits

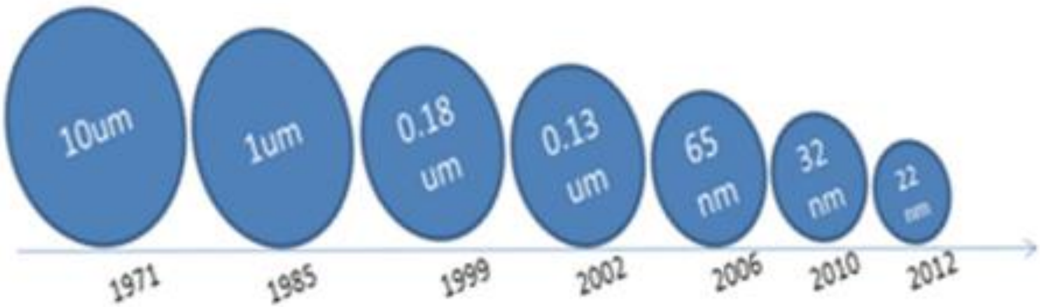


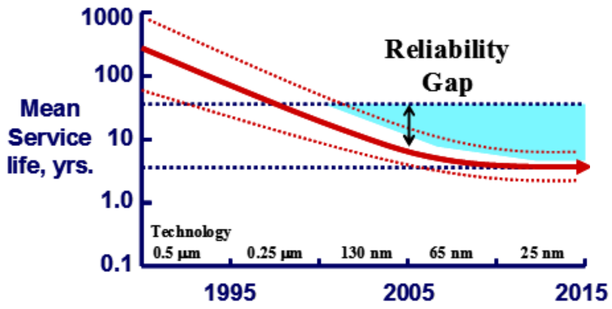
2) Larger, Higher Power, Hotter ICs

36x36mm Island BGA-1148



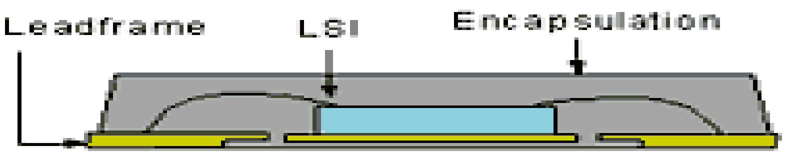
3) Smaller IC Technology Node/Feature Sizes Reduce Durability / Increase Failure Risks

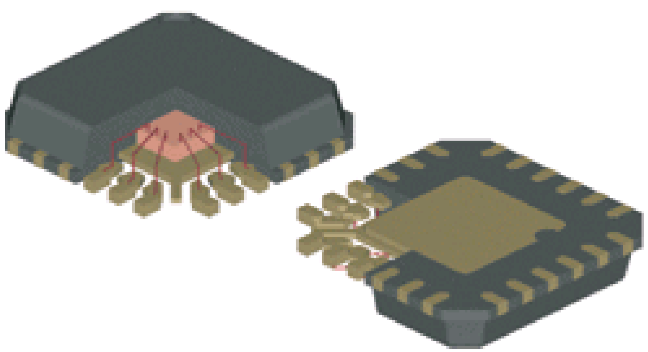


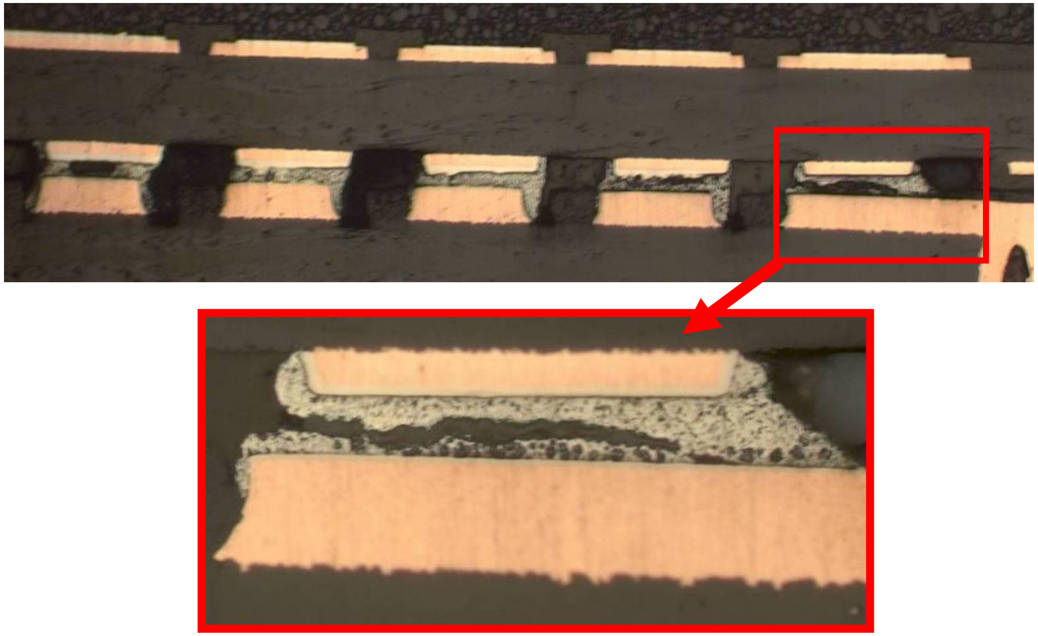



# 1) Flat No Lead IC

- The thin IC package results in a low (Silicon die dominate) Coefficient of Thermal Expansion (CTE ~4-6 ppm/°C) a large difference from the 14-17 ppm/°C CTE of printed circuit boards FNL ICs are soldered to.
- Large CTE difference combined with the thin solder joint results in a high sheer force that reduces the number of thermal cycles the IC can endure before solder attachment fatigue circuit failures occur.



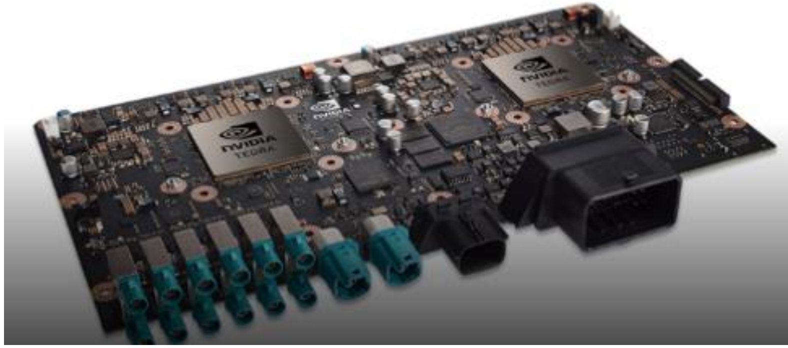


March 4th, 2018


Ford Brings Self-driving Cars To Miami

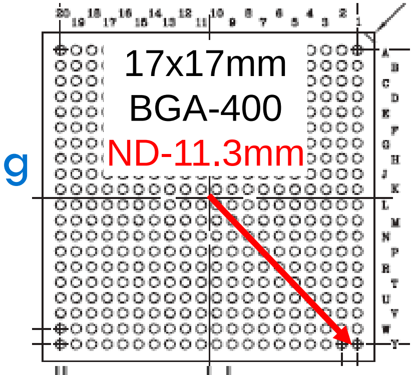
# 2+3) Emerging Smart Vehicle:

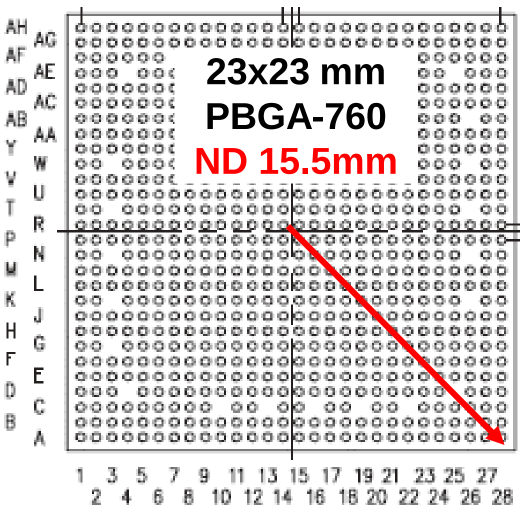
- Emerging Smart Vehicles Require Very Powerful Processing & Communication Modules
  - Parallel Processor / GPUs / AI
  - Ethernet controller
  - Cell modem
  - Wi-Fi controller
  - Data storage
  - Human Machine Interface (HMI)
    - Display, Touch Screen, Gesture Recognition
- The Large Super ICs these Features Require, Further Aggravate the CTE Mismatch Problems In Automotive Electronics

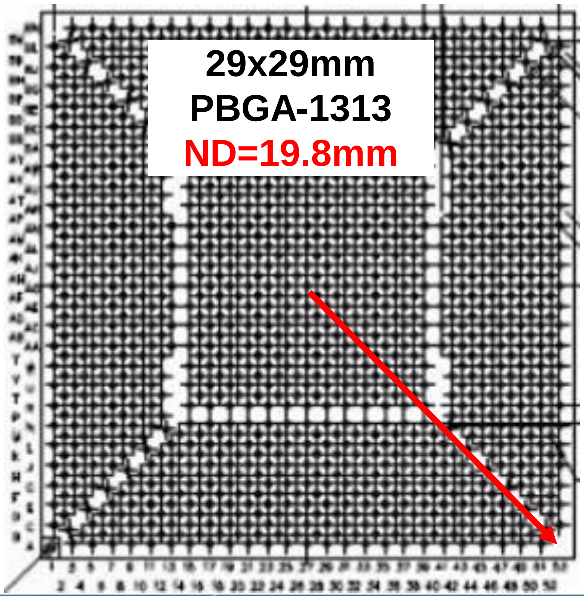



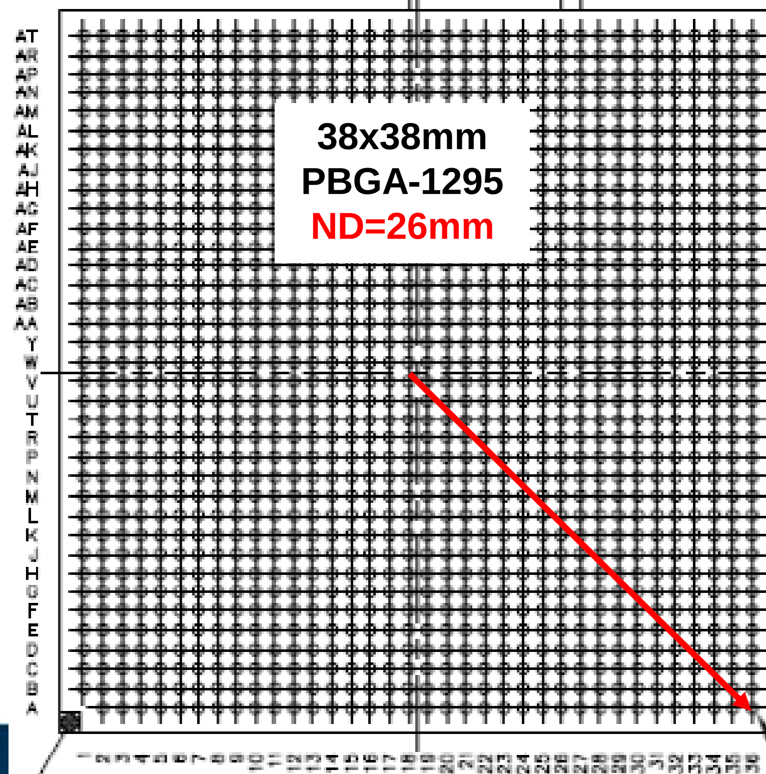
## 2) Reliability-Durability Challenges from Larger, Higher Powered, Hotter Running ICs w/Smaller Solder Balls

- Challenges from the opposite end of the IC size scale are appearing in the larger, powerful ICs (for autonomous vehicles & telecom).
  - Can have higher power dissipation self heating temperatures.
  - Longer neutral diagonal distance also results in high sheering stresses
  - Smaller solder balls for higher density I/O.
    - Increase thermal expansion/ contraction cycling solder fatigue risks.



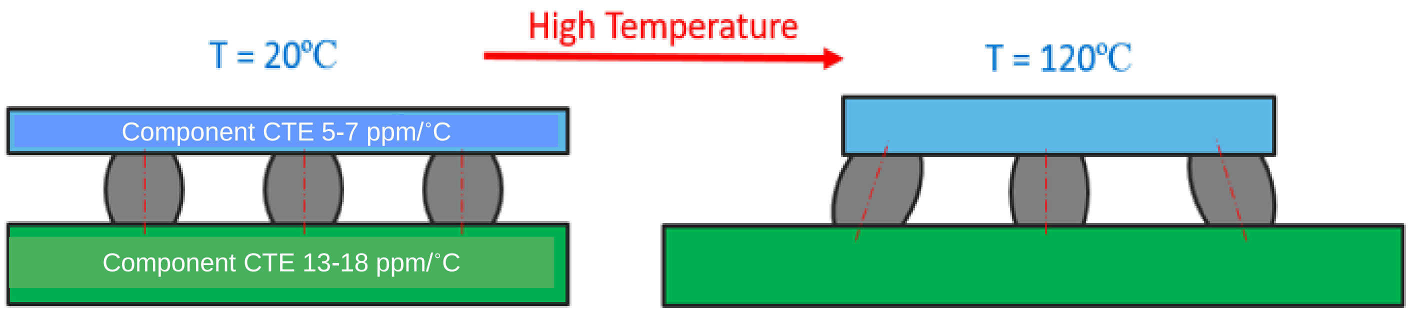



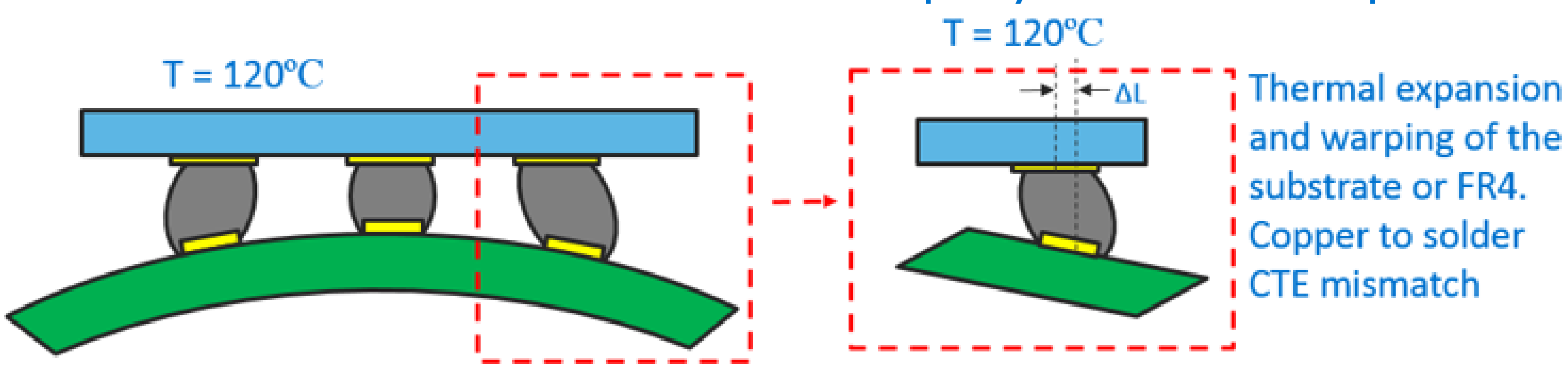



# 1+2) Stresses that Drive Electrical Component Solder Attachment Fatigue Failures

- In Plane CTE Mismatch -> Solder Under Compressive Shearing Loads

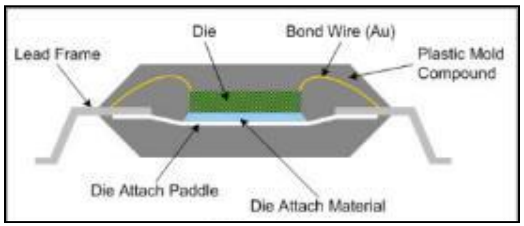


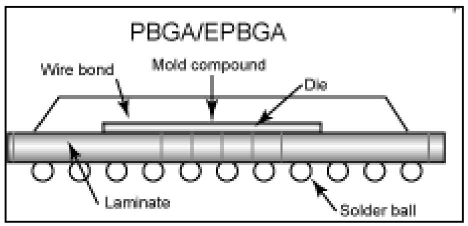

- In Plane CTE Mismatch + Micro Warpage
  Combined Shear with Tensile Loads That Rapidly Pulls Solder Apart

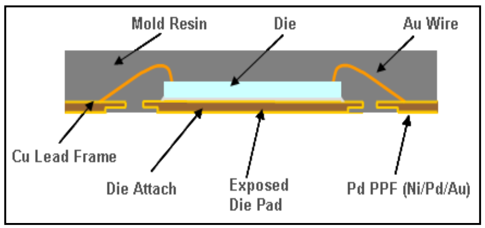


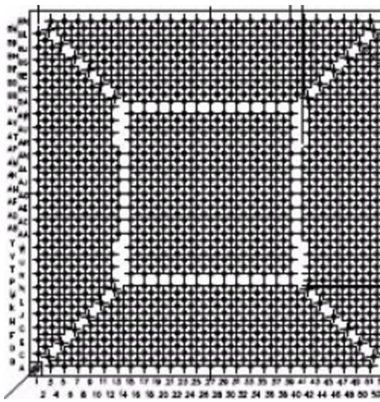
# 2+3) Comparative IC Package Failure Risks - Thermal-Mechanical Cycling Solder Fatigue

- Without a flexible terminal lead to absorb thermal Expansion/Contract motions, a high amount of thermal expansion stress is applied to the low profile under body solder joints, which accelerate solder fatigue failure.



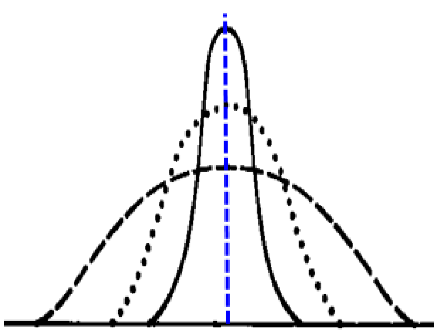



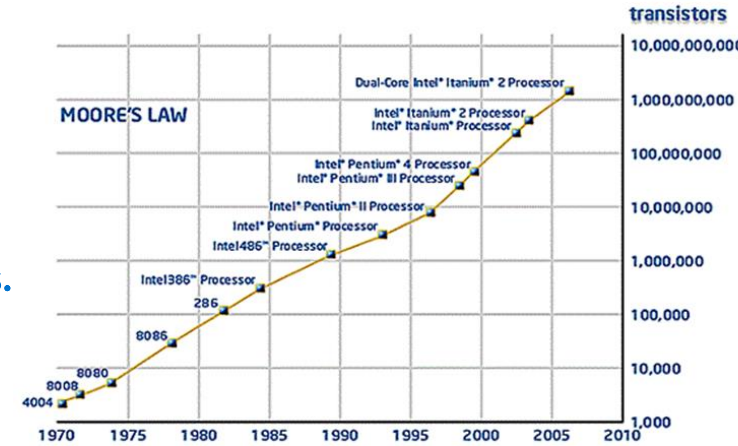



**Gull Wing Leaded QFPs >10,000 cycs.** → **Historic BGAs: (11x11mm BGA144) 3,000-8,000 cycs.** → **FNL CSP: 1,000-3,000 cycs.** → **Emerging 29x29mm BGA 1313 820 cycs. -40 to +85C**

| Package Type | Typ. Thermal Cycles to Failure (-40C to 125C) | Typ. Thermal Cycles to Failure (-40C to 85) |
|---|---|---|
| QFP | >10,000 | |
| Hist. BGA | 3,000 – 8,000 | |
| QFN | 1,000-3,000 | |
| Large BGA | | 820 |



## 3) Solid State Wearout Failure Mechanisms Becoming a Concern Again Due to Smaller Feature Scaling on High Density ICs



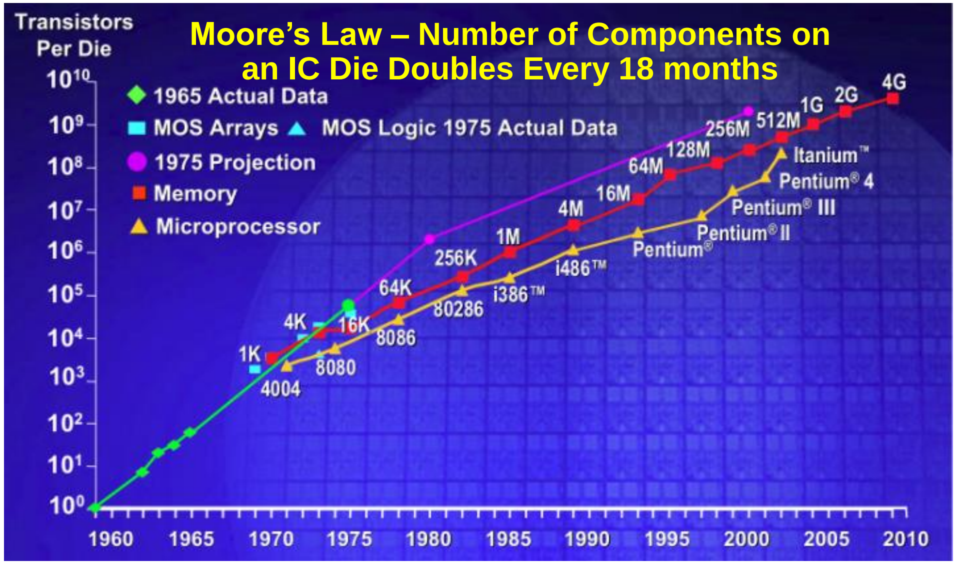

- 1960 Era Semiconductor & ICs had usage life of only a few thousand hours due to solid state wearout mechanisms.
  - As wearout mechanism were discovered, designs evolved to mitigate their effects
  - ICs grew to have millions to billions of operating hours of life.

- Today's High performance GPUs & AI ICs are fabricated using leading edge lithography tech. Now at 10nm Features & Getting Smaller)
  - The rapid IC advancement outpaces efforts to collect empirical data on life limits.
  - New lithography processes are introduced before reaching maturity increasing the risks of quality defect and resulting in shorter services lives.

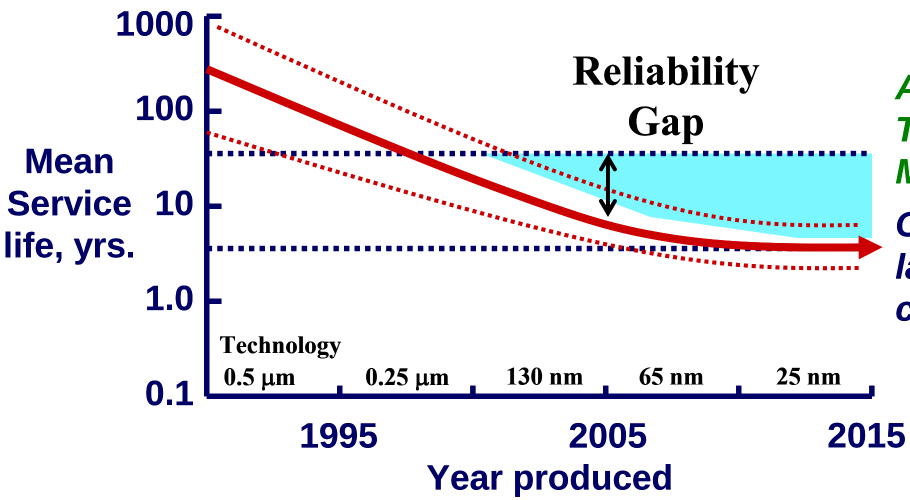
Photo: Darryl Bautista/Feature Photo Service/IBM

**Smallest So Far:** IBM made the first 7-nanometer-node test chips. There's little room to shrink further.

# IC Node Scaling Reduction in Advanced ICs Leading to the Return of Semiconductor Wear Out Mechanisms Concerns



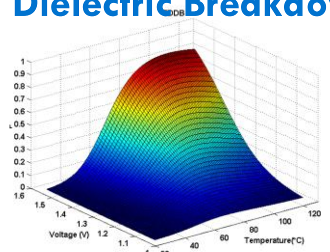

IC Scaling (65→45→32→22→14nm→..)
Smaller Feature Sizes & Isolation Spacing
Projected to Increase
Semiconductor Failure Rated and
Shorten Service Lifetimes



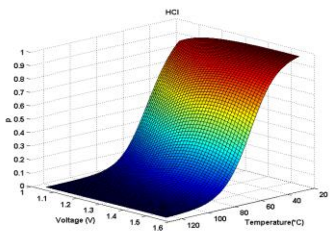

*Airplanes*
*Telecom*
*Medical*

*Computers*
*laptop/palm*
*cell phones*

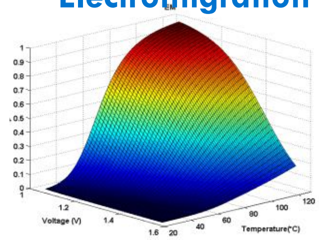
**Time Dependent Dielectric Breakdown**



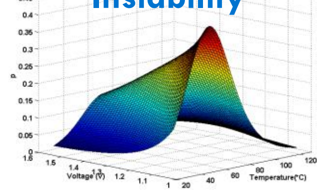
**Hot Carrier Injection**



**Electromigration**



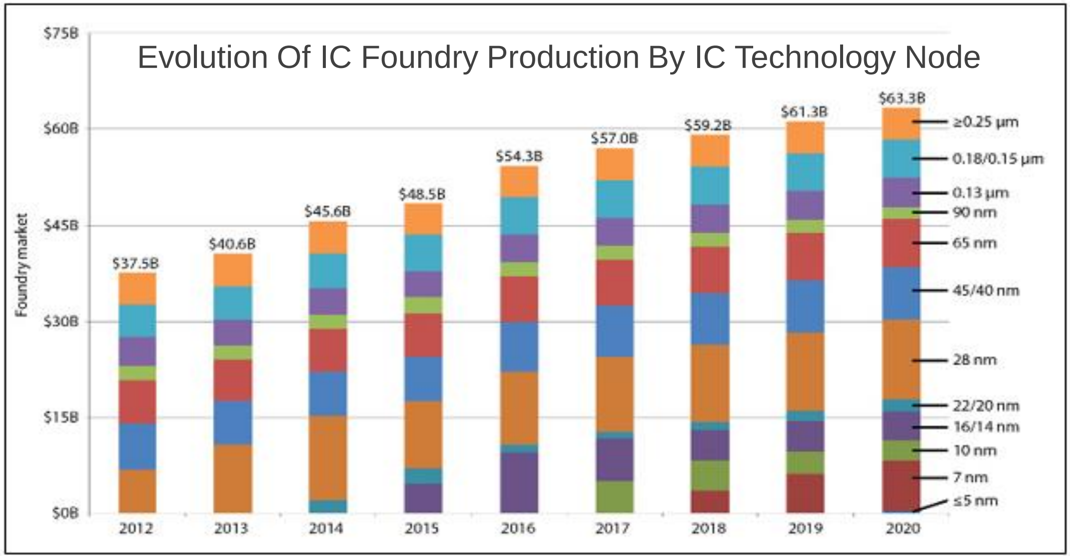
**Neg. Bias Temp. Instability**



# IC Technology - Node Evolution

- IC technology nodes are rapidly shrinking in accordance with Moore's law
  - The max number of transistors in ICs doubles approximately every 2 years, producing faster more powerful ICs as technology advancements produce smaller transistors, pack tighter together.
    - Mass production of 10nm ICs started in 2017.
    - 7nm ICs are tooling up to start mass production in 2018.
    - 5nm ICs expected by 2020.

Chart of Dollar Value of Historic & Projected IC Production by IC Technology Node
Source: [http://www.electronicdesign.com/industrial-automation/2017-will-be-b-i-g](http://www.electronicdesign.com/industrial-automation/2017-will-be-b-i-g)




  - Advanced ICs are 1st used in low stress, short life consumer electronics (i.e. Smart Phone & Tablets).
  - Rapid migration of advanced consumer grade ICs to HI-REL automotive is expected to be driven by the high processing & memory needs of Telecom, Safety & Self Driving Tech.

# USAF HiREV - Led Defense & Aerospace Research into Life Limited Advance ICs

HiREV

AIR FORCE RESEARCH LABORATORY

*Integrity ★ Service ★ Excellence*

**National High Reliability Electronics Virtual Center (HiREV) Program Update**

Daniel Marrujo
HiREV Liaison
The Defense Microelectronics Activity/MECA

# 3) Automotive IC Failure Risk Case Study
## - IC Supplier Define FIT (Failures per Billion Operating Hour) Rating

### IC 1 - Flash Memory (20nm) Supplier's Over All FIT Rating is: 28

| | Test Procedure / Conditions | Test Method Referenced | Duration or Level | Results # Lots | Results Failed / Tested |
|---|---|---|---|---|---|
| Reliability Level Tests | HIGH TEMPERATURE OPERATING LIFE<br>See below table for conditions. | JESD22-A108 | 168 hrs<br>504 hrs<br>1008 hrs | 3 | 0 / 231<br>0 / 231<br>0 / 231 |
| | PROGRAM ERASE CYCLING and<br>HIGH TEMPERATURE DATA RETENTION (NAND ONLY)<br>3.3V Vcc, distributed cycling at 85°C, post cycling bake temp equivalent to 55°C for 1 year/5 year. | JESD47 | Cycling<br>1 year<br>5 year | 3 | 0 / 231<br>0 / 231<br>0 / 231 |
| | PROGRAM ERASE CYCLING and<br>LOW TEMPERATURE DATA RETENTION (NAND ONLY)<br>3.3V Vcc, distributed cycling at 25°C, post cycling bake temp at 25°C. | JESD47 | Cycling<br>500 hrs | 3 | 0 / 231<br>0 / 231 |
| | HIGH TEMPERATURE STORAGE LIFE<br>150°C, no bias | JESD22-A103 | 168 hrs<br>504 hrs<br>1008 hrs | 3 | 0 /231<br>0 / 231<br>0 / 231 |

**Overall FITs Estimation**

| Parameter | Component NAND | Component uC |
|---|---|---|
| *Stress Device Hrs* | 232848 | 735000 |
| *Stress Temperature (°C)* | 125 | 125 |
| *Stress Voltage (V)* | 4.2 | - |
| *Operating Temperature (°C)* | 50 | 55 |
| *Operating Voltage (V)* | 3.3 | - |
| *Ea (eV)* | 0.6 | 0.7 |
| *ß ($V^{-1}$)* | 3.3 | - |
| *AF overall* | 1133 | 78 |
| *Pn* | 0.916 | 0.916 |
| *Number of components* | 4 | 1 |
| FITs | 12 | 16 |
| Overall FIT Rate | | 28 |

### IC 2 & 3 Controllers (20nm) Supplier's Overall FIT Rate is: 28

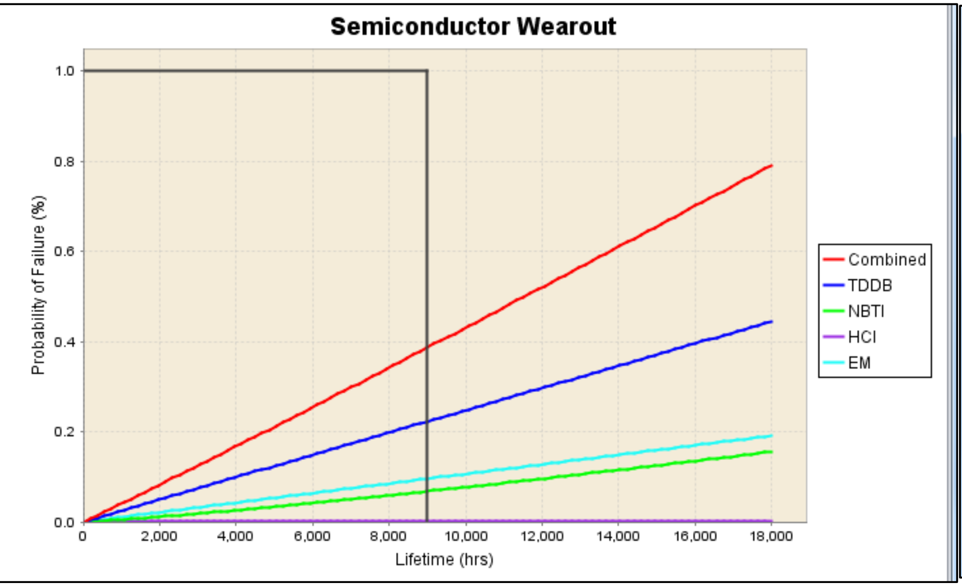
| Test | # | Reference | Test Conditions | Lots | S.S. | Total | Results SS/Pass/Fail | Comments: (N/A=Not Applicable) |
|---|---|---|---|---|---|---|---|---|
| TEST GROUP B — ACCELERATED LIFETIME SIMULATION TESTS | | | | | | | | |
| HTOL | B1 | JESD22 A108 | High Temp Operating Life: (Test @ Rm/Cold/Hot)<br>Stress conditions: 125C, 1.26V internal Vdd, 1008 hrs<br>Typical operating conditions: (50C, 0.96V internal Vdd at 1.1V external Vdd): 16 FITs<br>Ea=0.5eV, B=7, AFOVERALL=241, Pn=0.916 Device Hrs=2.328x10^5 | 3 | 77 | 231 | 0 of 231 | See note 2 |
| ELFR | B2 | AEC-Q100-008 | Early Life Failure Rate: (Test @ Rm/Hot)<br>Stress conditions: 125C, 1.26V internal Vdd, 48 hrs<br>Typical operating conditions: (50C, 0.96V internal Vdd at 1.1V external Vdd): 16 FITs<br>Ea=0.5eV, B=7, AFOVERALL=241, Pn=0.916 Device Hrs=2.408x10^5 | 3 | 800 | 2400 | 0 of 5016 | See note 2 |
| EDR | B3 | AEC-Q100-005 | NVM Endurance & Data Retention Test: (Test @ Rm/Hot) | 3 | 77 | 231 | of | N/A |

- Suppliers FIT Failure Rates are:
  - 28 per billions population operating hrs. for IC1
  - 16 per billions population operating hrs. for ICs2+3

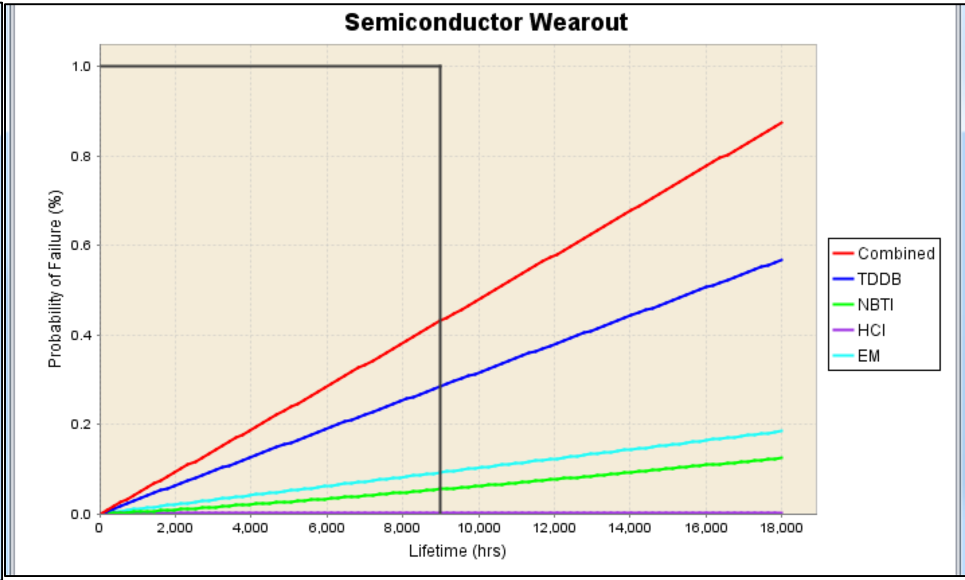
  Project to 9000 hrs. by $R=e^{-\lambda t}$ yields:
- $R = e^{-28x9000/1,000,000,000} = e^{-0.000252} = 99.975\%$
- $R = e^{-16x9000/1,000,000,000} = e^{-0.000144} = 99.986\%$
- **Life Time Reliability of the 3 ICs based on Supplier Defined FIT Rates is: 99.946% a Failure Risk of: 0.054%**

# 3) Automotive IC Failure Risk Case Study
## - Physics of Failure IC Failure Risks Calculator Results

### IC 1 - Flash Memory (20nm)




### IC 2 & 3 Controllers (20nm)




- IC1 Failure Risk at 10 years (at 900 hours/year) is ~0.387% (Reliability = 99.61%)
- IC2+3 Failure Risk at 10 years (at 900 hours/year) is ~0.435% (Reliability = 99.54%)

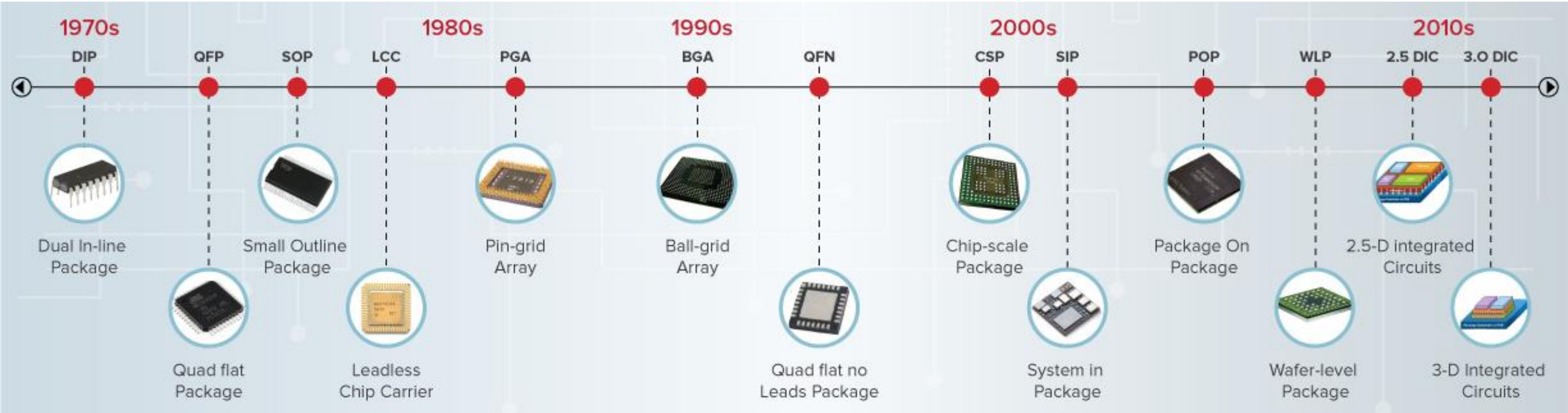
- **Combined Failure Lifetime Risks of the ICs to the Module is ~1.31% (R = 98.69%)**
  - **This PoF Calculated Failure Risk for the three 20nm ICs is 24.6 times higher than the Failure Risk produced by using the supplier's defined FIT rates which does not account for the differences of sub 50 nm failure mechanisms.**
  - **Failure Risk differences will be even greater for 10nm, 5 nm . . . ICs**

  www.DfRsolutions.com DfR Solutions RELIABILITY DESIGNED & DELIVERED

# Conclusions - E/E Technology Rapidly Evolves

- Each New Generation of E/E Tech Has Different Failure Risks & Failure Rates Than the Previous Generations.
  - Thus Actuarial Historical MTBF Metrics/FIT Failure Rates from the Last Decade, Can Not Accurately Predict the Failure Risks / Reliability of Tomorrow's Next Gen E/E Technology.
- This is why Automotive Electronics is Increasing adapting Physics of Failure / Reliability Physics Methods for Their E/E Systems

## Evolution of Semiconductor Technology



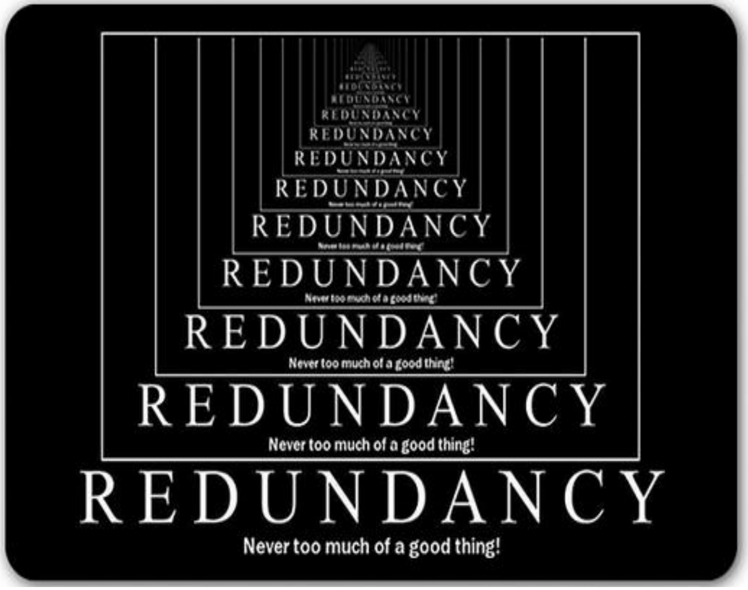

  

# PMHF Concerns

- There appear to be a lot of subjectivity in selecting values in the complex PMHF calculations & a lack of integrity of the source or traceability of the failure risk and time values used in these calculations.
  - How do we get confidence in the probability of a safety-related element fault/failure <u>occurring in conjunction with</u> a failure/fault of its safety mechanism.
  - In other words the process is susceptible to being manipulated (numbers picked out of the air) to produce any results that is desired.

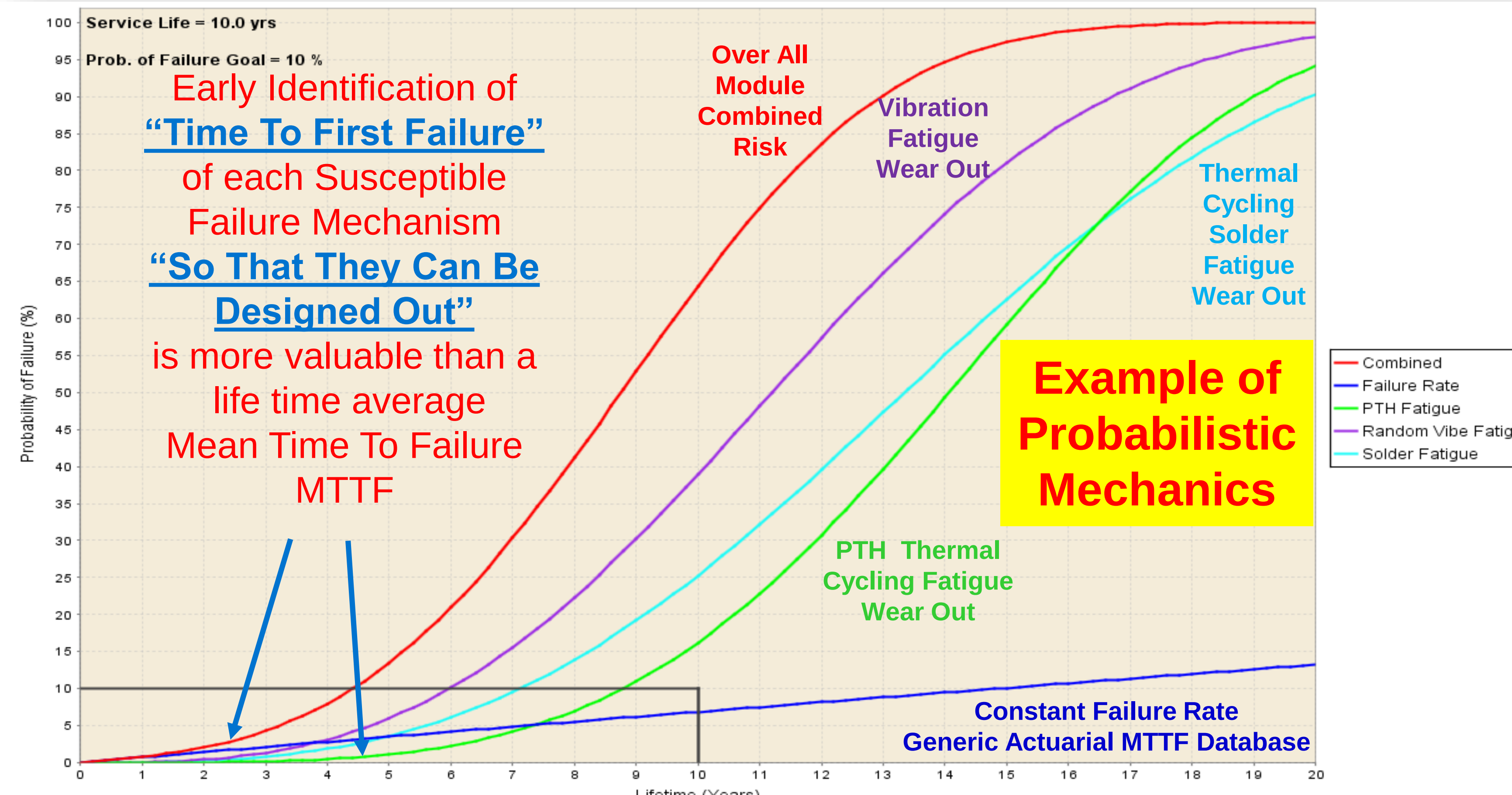
- If a safety-related functional elements have an excessive failure risk, then yes adding safety mechanisms <u>**"Which Is Already Industry Common Practice"**</u> makes sense.

- But if a safety element that's already enhanced with safety mechanism(s) still has a combined excessive failure risk "over the time to repair" period
  - Then what follow up action is needed or even possible
  - ISO-26262 Indicates that the safety community expects even more safety mechanism to be incorporated.



# Durability Simulations Produce Risk Life Curves for "Each Failure Mechanism" Tallied to Produce a Combined Life Curve for the Entire Module



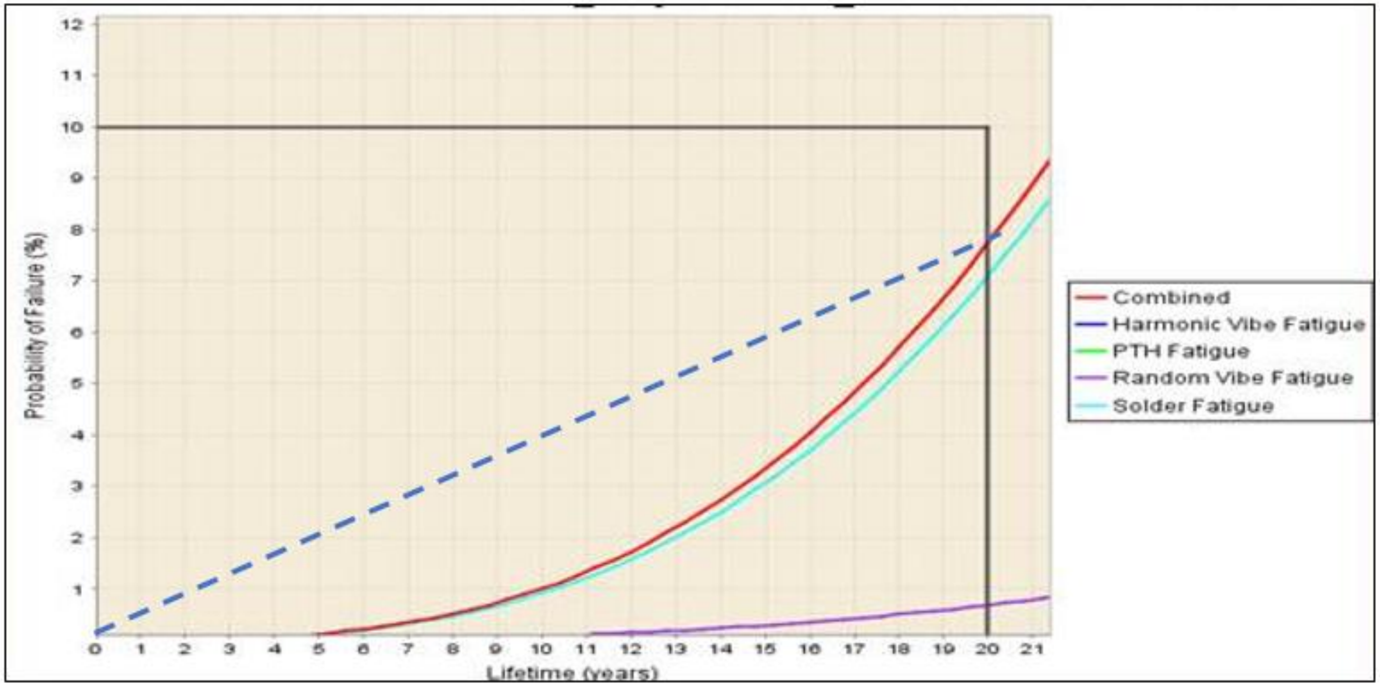

- More Accurate & insightful that a single averaged "Base Failure Rate" - approximated from obsolete failure rate data.

## How to Convert a Relevant Point from a PoF Durability Simulation Time Line Back to a Less Insightful Single Metric for use in PMHF Analysis

- (PMHF) is written in a manner that drives the need for one value.
- To convert a failure risk over time, life point from a durability simulation into a failure rate or MTBF metric all you have to do is apply the solve the classic reliability equation backwards for the failure rate Lambda of the MTBF/MTTF)

  - $R = e^{-\lambda t} = e^{-t/MTBF}$ and then $\ln R = -\lambda t$
  - Solving for the failure rate Lambda yields $\lambda = \ln R/-t$

- The failure risk probability at 20 years is F = 7.73% and R = 100% - F = 92.27%
- Dotted line illustrates the path of an "over simplified, hypothetical constant random failure rate would take to reach the same 20 year life failure risk point.
  - Assuming that "t" is the hours in 20 years
    = 20 yrs x 365.25 days/ year x 24 hours/day = 175,320 hours, then:
    - λ = ln R / -t = ln 0.927 / -175320 = -0.07580 / -175320
    - = 0.0000004324 failures per hour or 43.24 x 10-6 failures per hour and
    - MTBF = 1/ λ = 2,312,876.48 hours



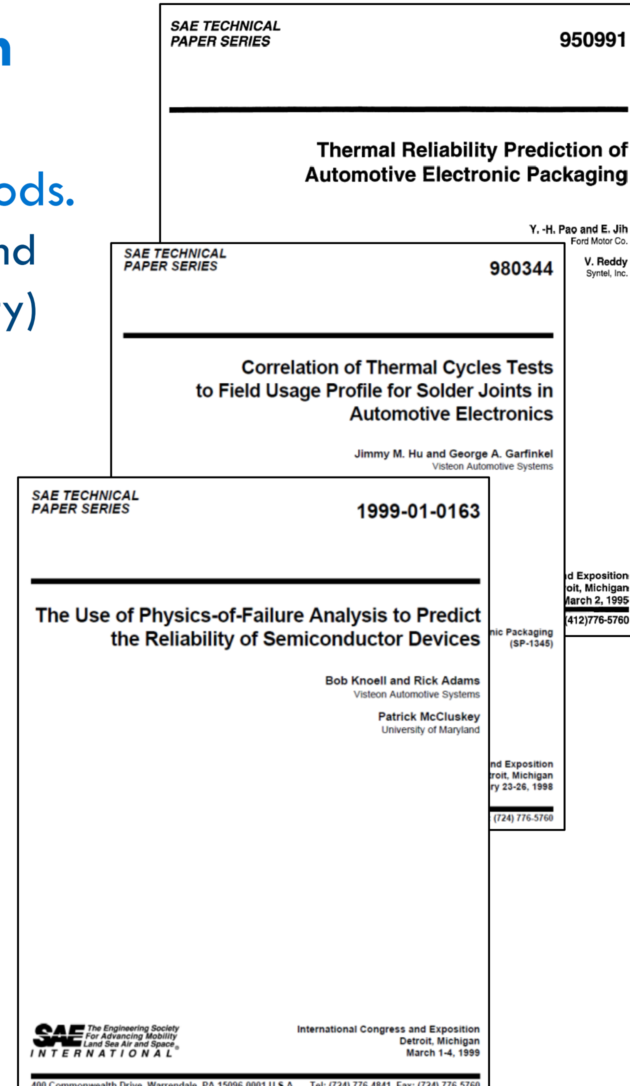

  

# Evolution of Ford's Product Reliability Paradigm

- Early 1990's decision was made to use 99th percentile customer usage conditions as E/E system requirements for
  - Temperature Reliability/Durability Tests
  - Vibration Reliability/Durability Tests
- In parallel one set of standard test flows were created for entire corporation
  - Test levels used were based on location of part in the vehicle
- Example: For vibration testing the F 250 truck "g" force levels are used on all E/E devices as a 'robustness action'.
  - RESULT:
    - Three to four years later, $200 to 300 savings in warranty "PER VEHICLE"
    - Streamlined test lab activities
    - Estimated lab test cost savings corporate wide $10 million+

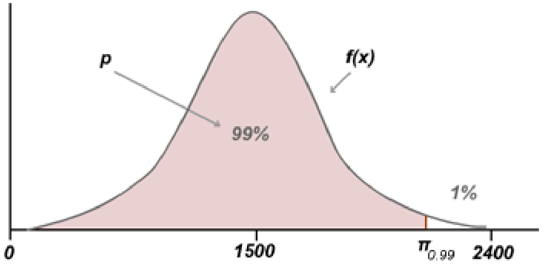
# Evolution of Ford's Product Reliability Paradigm

- Late 1990s Ford and their E/E Division (now Visteon) began to develop and implement Physics of Failure methods.
  - Hired Physics of Failure grads from the University of Maryland
  - Develop "Ford CAIR" (Computer Aided Interconnect Reliability) a CAE program for Solder Thermal Cycling & Vibration Fatigue Life Prediction
  - Developed PoF based "Key Life Tests"
    *(called Failure Mechanism Susceptibility Detection Testing at GM)*
    (ref: https://www.autoblog.com/2012/12/20/ford-key-life-test-advanced-plug-in-vehicle-batteries/)
    https://www.sae.org/publications/technical-papers/content/972587/
    *Reliability Predictions Using Probabilistic Methods and Key Life Testing*
  - Developed Design Rules, Worst Case Circuit Analysis and Lessons Learned Check Lists that were incorporated into Ford's Engineering Processes & Test Standards
- Result:
  - Eliminated all temperature/current-load related failures
  - Eliminated HALT & Statistically Significant Sample Sizes Testing
  - Reduced Warranty Cost & Increased Customer Satisfaction
  - Significant reduction in validation tests sample size and cost.



# Evolution of Ford's Product Reliability Paradigm

- Fords Reliability Paradigms switched to:
  - CUSTOMER USAGE: determine 99th percentile customer usage
  - STRENGTH OF TEST: implement 99th percentile customer usage
  - MISTAKE PROOFING: design tests & test flow to find and eliminate mistakes




- Tests were designed to **'KILL'** in order to:
  - Find Life Limits & Weak Links so they could be fixed
  - Resulted in a drastic reduction in sample size, test times & test costs.

- Focused Validation
  - Allows the test focus to be on what is new or changing
  - All test plans are tailored – No Exception.
  - Use of surrogate data where ever possible

# Evolution of Ford's Product Reliability Paradigm

- **Design Validation (DV):**
  - Test sample sizes reduced for 20 to 12
  - 6 for multi-environmental leg
  - 6 for Thermal Shock Endurance KLT
    - That was reduced from 1000 to 500 cycles
  - DV Test time reduced by 15 days.
- **Process/Production Verification (PV):**
  - Test sample sizes reduced from 26 to 12
  - 6 for multi-environmental leg
    - Test time reduced by 9 days
  - 6 for Thermal Shock Endurance
- Corporate Confidence in test robustness/effectiveness greatly increased.

# Evolution of Ford's Product Reliability Paradigm

$$R_c = (1-C)^{\frac{1}{(n+1)}} \qquad R = 1 - \frac{0.5 \times \chi^2_{(1-C,2(r+1))}}{n}$$

$$n = \frac{0.5 \times \chi^2_{(1-C,2(r+1))}}{1-R}$$

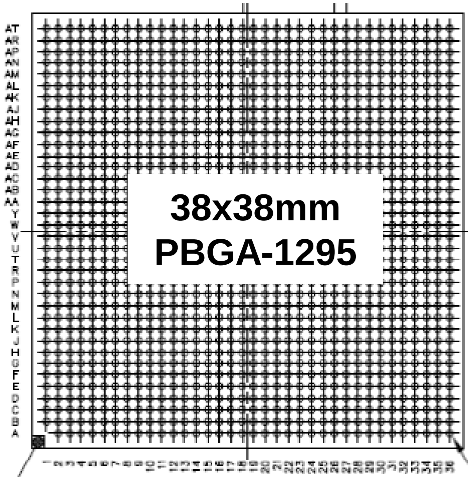
- **Classical View of Test Confidence**
  **- Bayes Success Run Theorem***
  - Defines the statistical relationship between:
    - Statistically Significant Sample Size,
    - Duration of Test Relative to Usage Life
    - Demonstrated Reliability &
    - Confidence in the Test Results.
  - But Bayes Theorem can not account for test stress relative to in service usage stress relative to the strength & capabilities of a product's materials.
    - Correlation of Test Stress Acceleration Factors requires Reliability Physics Durability Simulation applied in a "SAT -Simulate Aided Testing" or "SGT- Simulated Guided Testing" processes.


* Ref: TEXT BOOK: "Statistical Design & Analysis Of Engineering Experiments" by LIPSON & SHETH
SECT 5.4: Relationship Between Sample Size, Test Time, Confidence & Reliability - Using Bayes Theorem

# Ford's Partnerships with DfR Solutions

- **Benefits of Design for Reliability Knowledge & Using Sherlock ADA**
  - #1 Educating Ford's Suppliers in Harsh Environment Failure Risk Reliability Physics Analysis & DfR methodology.
    - Especially important as many new AI & Remote Sensor start up firms are entering the Automotive Supply chain with Autonomous Vehicle Technology. Such as Ford's new AV partnership with the Argo AI startup.
      - Ref: ***"An inside look at Ford's $1 billion bet on Argo AI"*** https://www.theverge.com/2017/8/16/16155254/argo-ai-ford-self-driving-car-autonomous

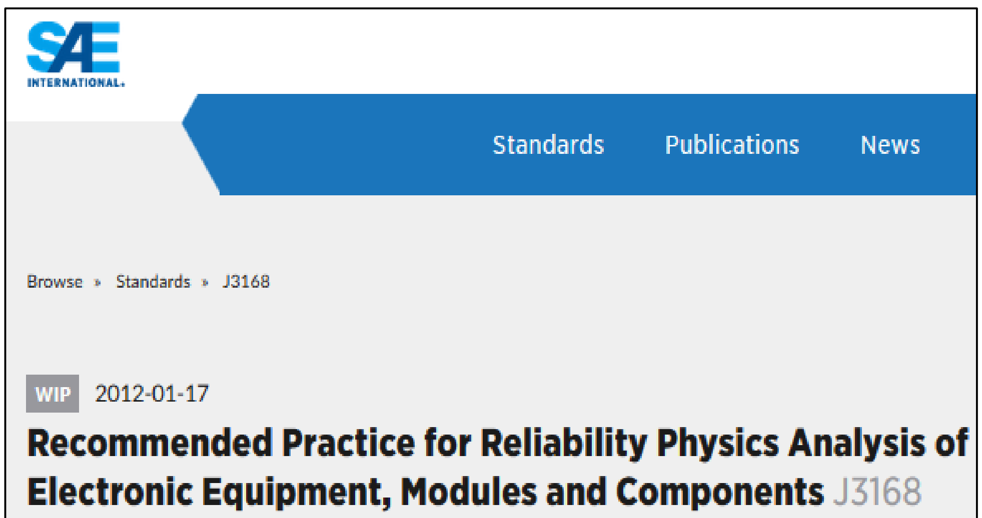
- 1st time pass on new ultra large BGA
- Ability to identify/eliminate poor PCB designs & poor PCB suppliers
- Knowledge for hardening/robustness of E/E products
- Improvements on all designs aspect (PCB & EE Components)
- Support for ISO 26262 Reliability/PMHF assessments
  - Reduce the need for redundancy to only where it is really needed
  - Expectations for future prognostic methods.
- **IC RELIABILITY MODELS (Sub 50 Nm Risks)**
  - Enable Working With IC Suppliers on Failure & Wearout Risks of New Advanced ICs.



# Ford's Partnerships with DfR Solutions – NEXT STEPS

- **Develop SAE J3168 – "Recommended Practice for Reliability Physics Analysis of Electronic Equipment, Modules and Components"**, *Ref: https://www.sae.org/standards/content/j3168/*
  - A new joint SAE Automotive & SAE Aerospace Standard To identify
    - Best practices for CAE Durability Simulation of Electrical, Electronic & Electromechanical (EEE) Equipment, Modules & Components used in the Automotive, Aerospace, Defense and other High-Performance (AADHP) industries.
  - This document will describe the baseline RPA process and will contain a series of appendices or sub-documents to describe the specific models and its implementation in a range of specific circumstances.



# Ford's Partnerships with DfR Solutions – NEXT STEPS

- SAE J3168 – Work in Progress Initial Outline

1 INTRODUCTION
2 SCOPE
3 APPLICABILITY
4 REFERENCES
5 DEFINITIONS, INITIALS, AND ACRONYMS
6 RELIABILITY PHYSICS ANALYSIS PROCESS
7 IMPLEMENTATION OF THE RPA PROCESS
8 BIBLIOGRAPHY

Appendix A: Structural Integrity - Circuit Board Mech. Stack up Analysis.
Appendix B: Structural Integrity - Thermal Mechanical Cycling Fatigue
Appendix C: Structural Integrity - Mechanical Vibration Fatigue
Appendix D: Structural Integrity - Mech. Shock Fracture
Appendix E: Structural Integrity - Repetitive Shock Fatigue.
Appendix F: Structural Integrity - Plated Through Hole Via Fatigue
Appendix G: Simulated Guided/Aided Test to Field Correlation
Appendix H: Sub 50nm Semiconductor Failure Risks Analysis
Appendix I. Use in ISO-26262 Functional Safety PMHF Risk Analysis
Appendix J. Use in Aircraft Equipment Certification

- J3168 will align with and cross reference the following existing SAE standards:
  - SAE J1211 - Handbook for Robustness Validation of Automotive Electrical/Electronic Modules
  - SAE J1879 - Handbook for Robustness Validation of Semiconductor Devices in Automotive Applications
  - SAE J3083 - Reliability Prediction for Automotive Electronics Based On Field Return Data
  - SAE J2940 - Use of Model Verification and Validation in Product Reliability and Confidence Assessments
  - SAE J2816 - Guide for Reliability Analysis Using the Physics-of-Failure Process
  - SAE ARP6338 - Process for Assessment & Mitigation of Early Wearout of Life-limited Microcircuits.
  - SAE ARP6379 - Processes for Application-Specific Qualification of Electrical, Electronic, Electromechanical Parts and Sub-Assemblies for Use in Aerospace, Defense, and High Performance Systems

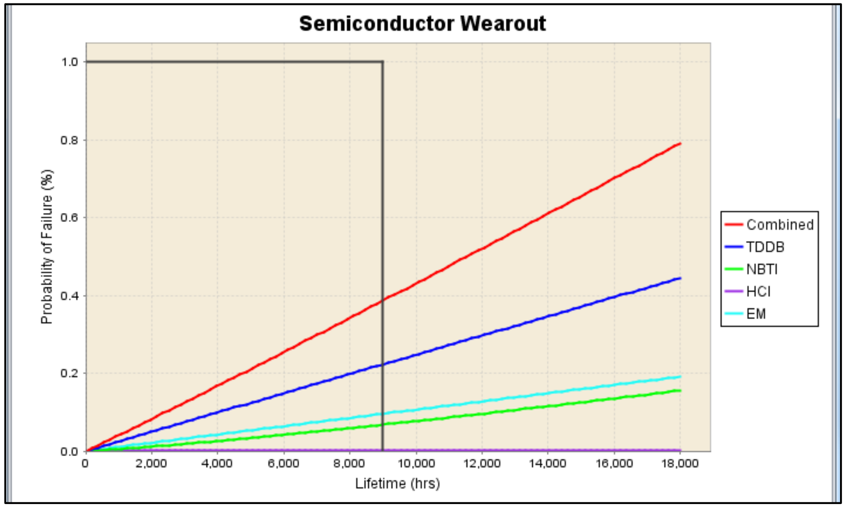
# Ford's Partnerships with DfR Solutions – NEXT STEPS

- **Thermal & Mechanical Durability Simulation to reduce test cycles & sample sizes**
  - For Both DV (Design Validation) and PV (Product Validation)
  - Evaluate if DV could evolve into and all CAE Virtual activity
  - Evaluate if vibration durability & shock testing can be replaced with modal resonance checks.

- **Enhancement to Sherlock to Support ISO-26262 PMHF Documentations.**
  - PMHF is performed on each ASIL B-C-D level critical sub-element of a system.
  - Need analysis performed on individual B-C-D level Sensor & Actuator I/O Circuits in addition to the complete PCBA.
  - With ability to manually add it wiring & sensor/actuator elements of the circuit external to the PCBA.
  - Ability to generate PMHF reports that will need to be maintained as part of Production Part Approval Process (PPAP) documentation, similar to today's FMEA documents.

# Ford's Partnerships with DfR Solutions

- **Benefits of Design for Reliability Knowledge & Using Sherlock ADA (Continued).**
  - **IC RELIABILITY MODELS (Sub 50 Nm Risks)**
    - Opportunity To Partner and 'Intelligently' Work With IC Suppliers To Project Failure Risk and Wearout of Current and New IC Designs
    - Assist With 'Real' Reliability Assessments
  - **Potential for future embedded prognostic to monitor life consumption of life limited sub 50 nm IC based on how each vehicle is being used.**



# Conclusion

- The ISO-26262 Vehicle System Function Safety Specification requires extensive effort to identify and address potential safety related faults and failure issues based on outdated 1950 era reliability paradigms.
- Today's "Design For Reliability" community feels that a Reliability Physics focuses on eliminating or mitigating "ALL" faults and failure issues is simpler and more effective.
  - After all if you eliminate all failure and faults risks, not only do you produce a safe vehicle, but you also get a vehicle that is highly reliable in all categories which:
    - Improves Customer Satisfaction & Brand Loyalty
    - Build Brand Image
    - Cuts Warranty Costs
    - In Addition to Safety

# Thank you for your attention.
# Any questions?