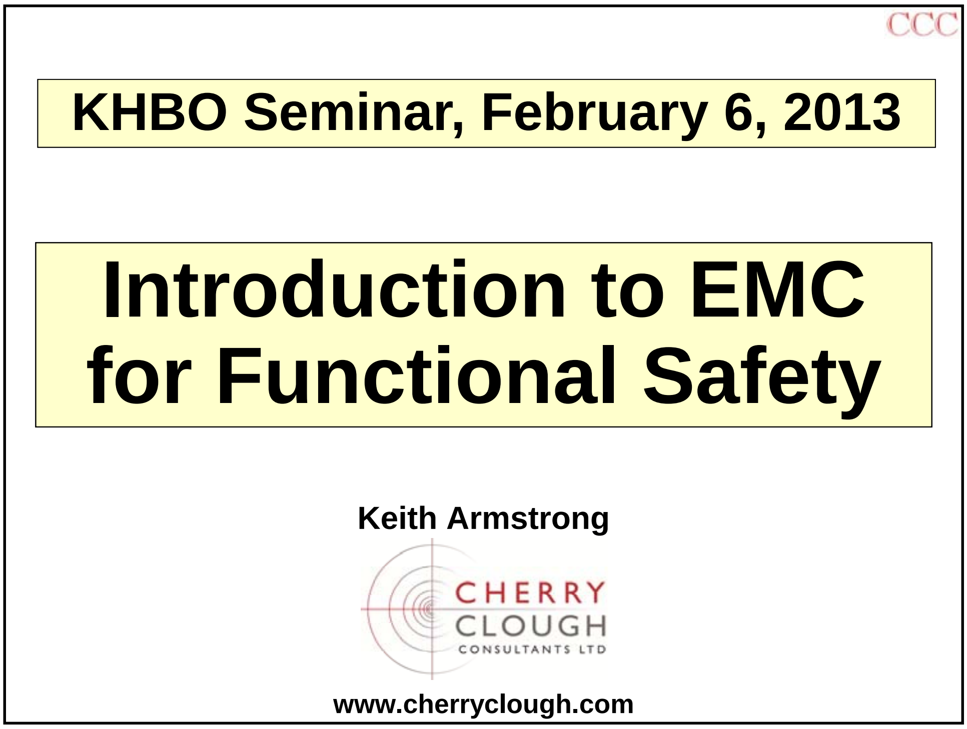


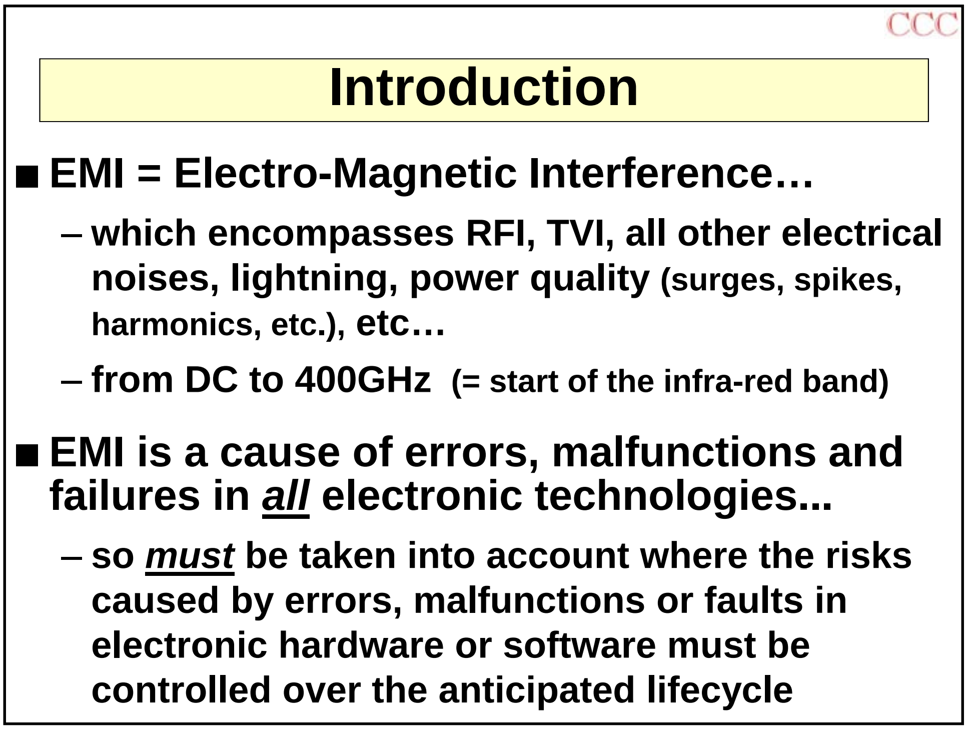
KHBO Seminar, February 6, 2013

Introduction to EMC for Functional Safety

Keith Armstrong

CHERRY CLOUGH CONSULTANTS LTD

www.cherryclough.com



Introduction

- EMI = Electro-Magnetic Interference…
  - which encompasses RFI, TVI, all other electrical noises, lightning, power quality (surges, spikes, harmonics, etc.), etc…
  - from DC to 400GHz (= start of the infra-red band)
- EMI is a cause of errors, malfunctions and failures in ***all*** electronic technologies...
  - so ***must*** be taken into account where the risks caused by errors, malfunctions or faults in electronic hardware or software must be controlled over the anticipated lifecycle

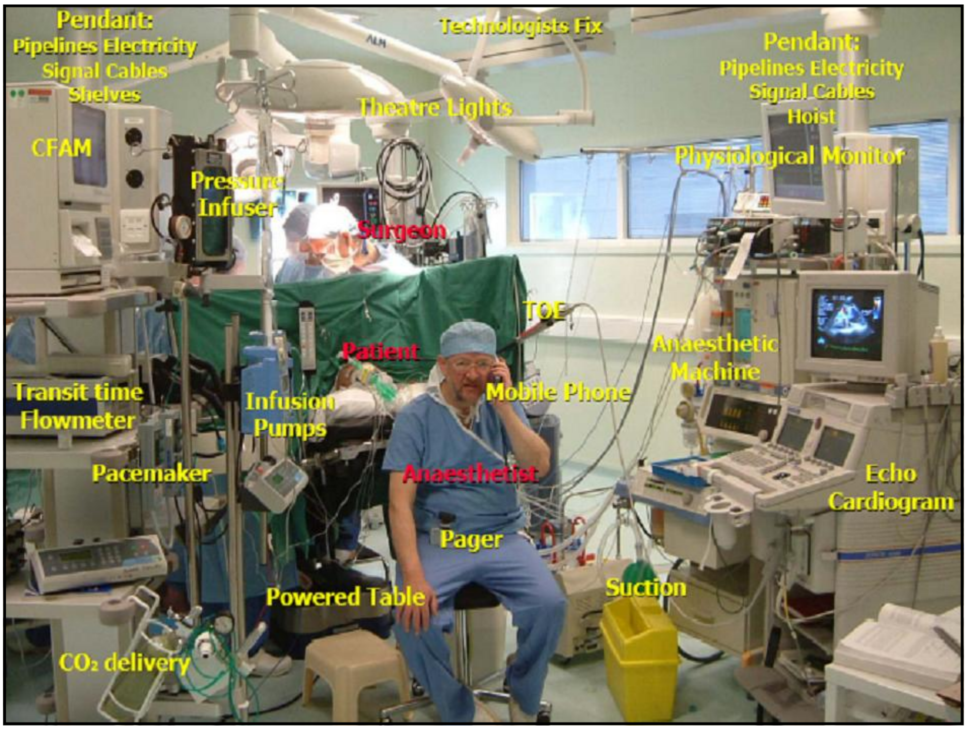
EMC = electromagnetic compatibility — the engineering discipline of controlling EMI

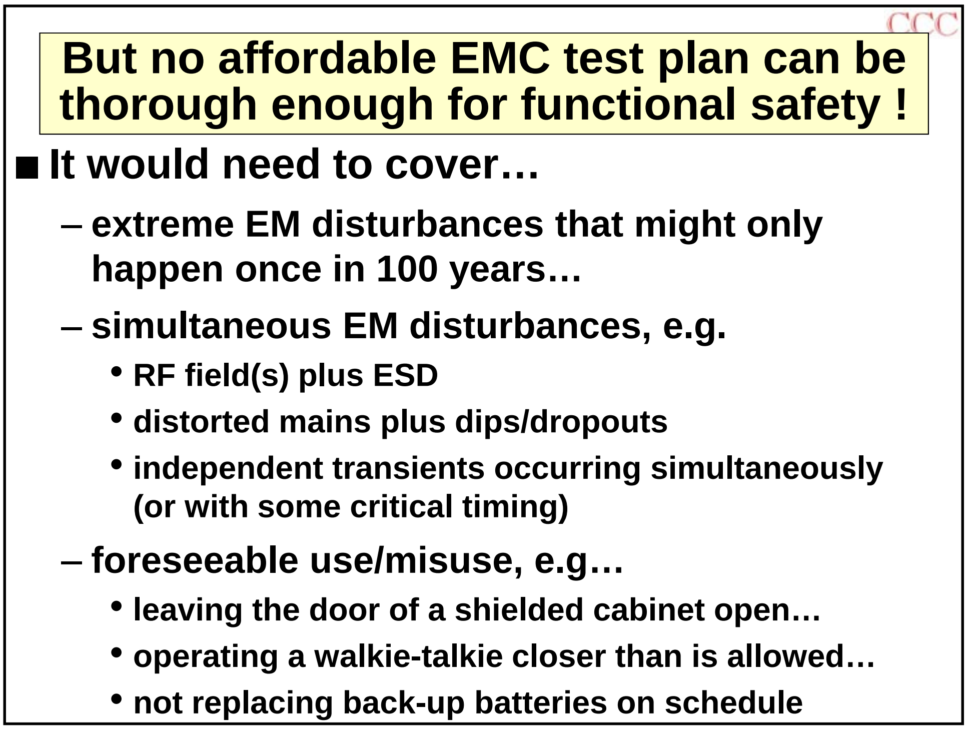
- Most Functional Safety engineers and assessors leave the EMC to EMC test labs…
  - who test to EMC Directive immunity standards…
  - which aim to cover 80% of normal EMI events, (which is not even the start of the SIL 1 range)…
  - and ignores low-probability EMI, which will occur during the safety system's lifecycle
- Result?
  Most (all?) functional safety system designs and their independent safety assessments do not adequately control EMI!

The following slide is a photograph of an operating theatre in *typical* use...

- provided by Dr David H T Scott
  (the guy on the phone)…
  - Pask Certificate of Honour,
    Consultant Cardiothoracic Anaesthetist and Intensive Care Specialist, Department of Anaesthetics,
    The Royal Infirmary of Edinburgh,
    EH16 4SA, UK. Mobile: 07788 415 489
  - Dr Scott retains the copyright of this photograph

- The EM environment in this room is *very* different from that assumed by the medical EMC standard IEC/EN 60601-1-2 for its immunity tests!





But no affordable EMC test plan can be thorough enough for functional safety !

- It would need to cover…
  - extreme EM disturbances that might only happen once in 100 years…
  - simultaneous EM disturbances, e.g.
    - RF field(s) plus ESD
    - distorted mains plus dips/dropouts
    - independent transients occurring simultaneously (or with some critical timing)
  - foreseeable use/misuse, e.g…
    - leaving the door of a shielded cabinet open…
    - operating a walkie-talkie closer than is allowed…
    - not replacing back-up batteries on schedule

But no *affordable* EMC test plan can be thorough enough for functional safety ! continued…

- ageing and wear; four types of corrosion; shock & vibration, etc. that can degrade EM characteristics over the lifetime, e.g…
  - ICs' EM immunity generally gets 10dB *worse* over the first 4 years of operation…
  - some *fully IEC-compliant* X2 capacitors lose 10% value every 1000 hours operation, e.g. 100nF can be 9nF after 3 years continuous use, completely altering the performance of filters or transient suppression…
  - shielding has been seen to degrade by 60dB in less than a year, due to corrosion from an especially aggressive climatic environment

But no *affordable* EMC test plan can be thorough enough for functional safety ! continued…

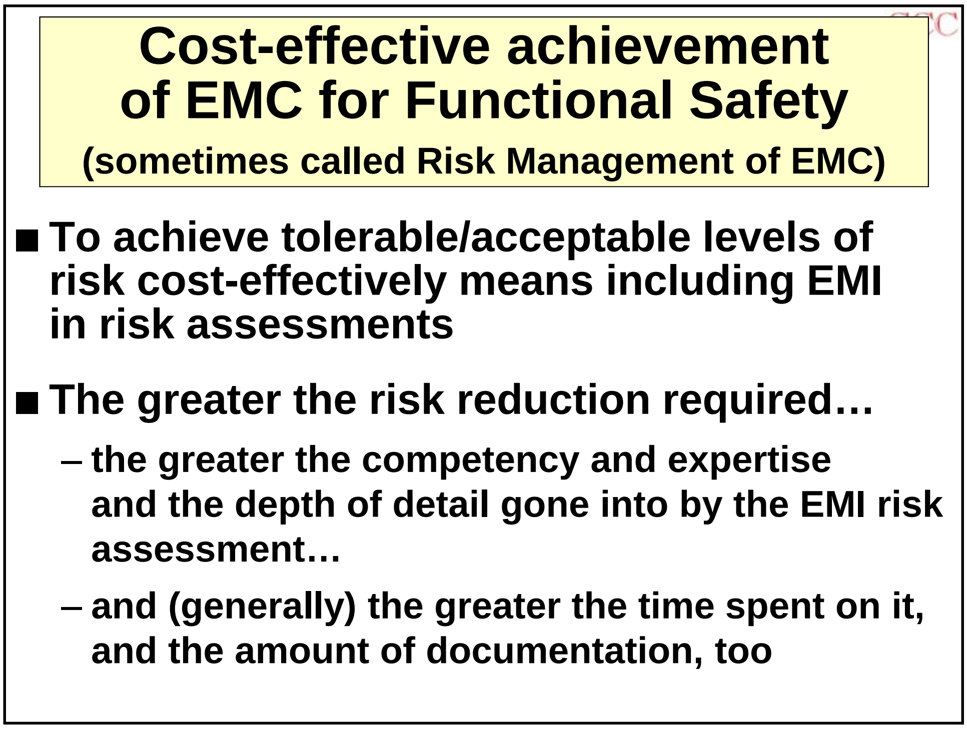
- foreseeable faults, e.g…
  - loosened filter ground bonds…
  - loosened joints between shielding parts…
  - intermittent/failed contacts, solder joints, etc.
- effects of temperature, loading, mains voltage…
  - variations *within a filter's maximum ratings* have been seen to reduce its attenuation by 20dB compared with when EMC tested
- effects of supply impedance on filters…
  - can cause up to 20dB gain to appear in the frequency range where attenuation is achieved on the standard EMC tests

Introduction continued...

- A comprehensive test plan would have to cover foreseeable *combinations*, too…
    - e.g. a corroded RF shield, plus aged ICs with 10dB more susceptibility, plus a too close walkie-talkie…
  - – the test plan would 'explode' – needing many years (possibly decades) to complete
- So we need some other way of proving adequate design confidence for the SIL...
  - – in its reasonably foreseeable worst-case "electromagnetic environment"...
  - – for its anticipated lifecycle and physical/climatic/user environments

IEC 61508 Ed.2:2010 makes EMI control and assessment mandatory…

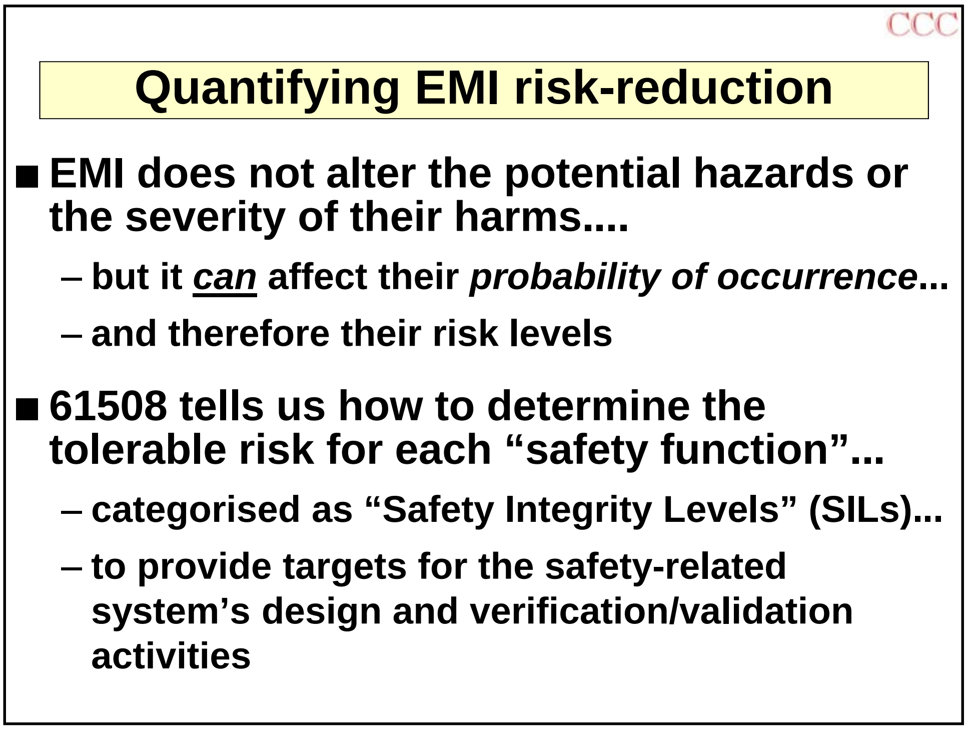
- – by requiring compliance with IEC TS 61000-1-2 Ed.2:2008 – "EMC for Functional Safety"…
    - for which there is a very practical IET Guide at www.theiet.org/factfiles/emc/index.cfm...
- – which requires EMC design to be based upon the results of risk assessment…
- – then the design verified/validated using a wide range of techniques (including, *but not limited to,* EMC immunity testing)



Cost-effective achievement of EMC for Functional Safety

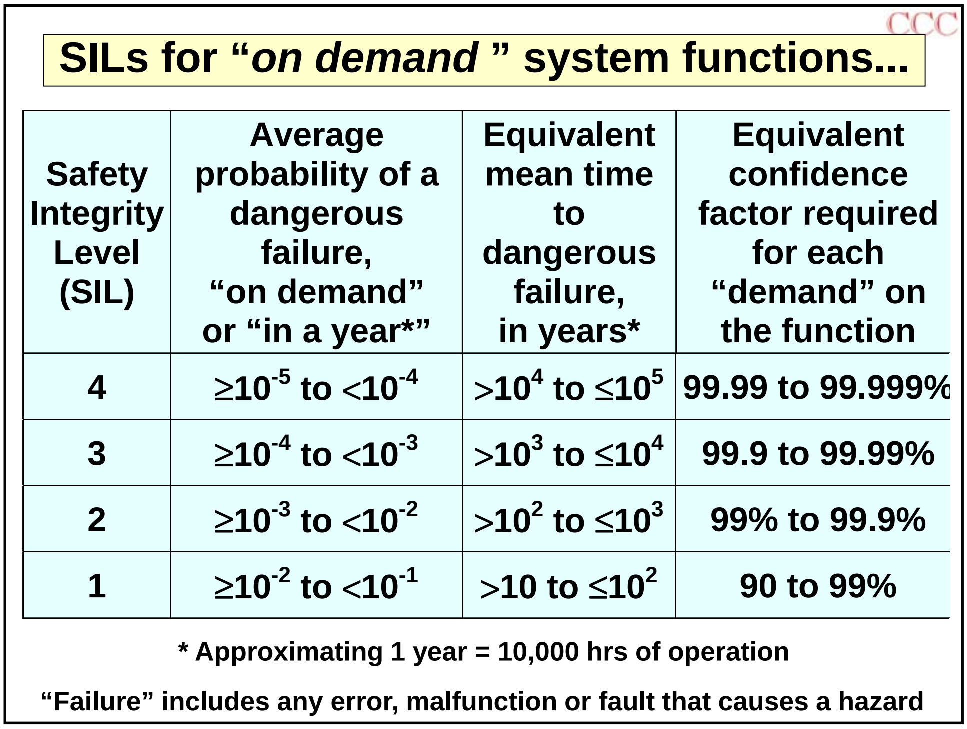
(sometimes called Risk Management of EMC)

- **To achieve tolerable/acceptable levels of risk cost-effectively means including EMI in risk assessments**
- **The greater the risk reduction required…**
  - **the greater the competency and expertise and the depth of detail gone into by the EMI risk assessment…**
  - **and (generally) the greater the time spent on it, and the amount of documentation, too**



Quantifying EMI risk-reduction

- **EMI does not alter the potential hazards or the severity of their harms....**
  - **but it *can* affect their *probability of occurrence*...**
  - **and therefore their risk levels**
- **61508 tells us how to determine the tolerable risk for each “safety function”...**
  - **categorised as “Safety Integrity Levels” (SILs)...**
  - **to provide targets for the safety-related system’s design and verification/validation activities**

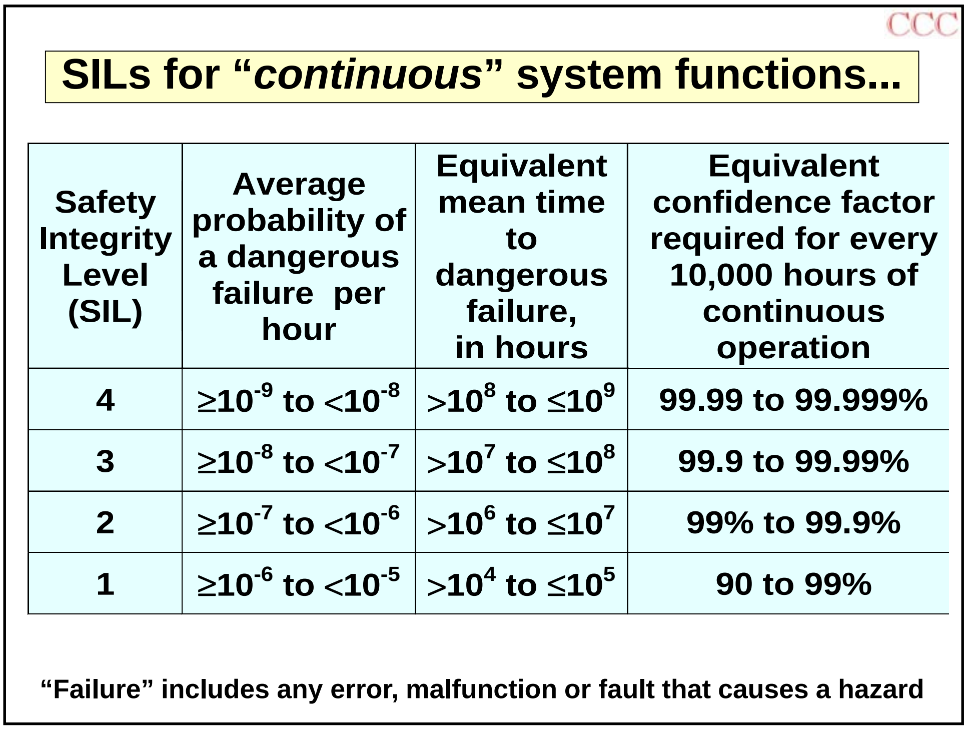


SILs for "*on demand* " system functions...

Safety Integrity Level (SIL)	Average probability of a dangerous failure, "on demand" or "in a year*"	Equivalent mean time to dangerous failure, in years*	Equivalent confidence factor required for each "demand" on the function
4	$\geq 10^{-5}$ to $<10^{-4}$	$>10^{4}$ to $\leq 10^{5}$	99.99 to 99.999%
3	$\geq 10^{-4}$ to $<10^{-3}$	$>10^{3}$ to $\leq 10^{4}$	99.9 to 99.99%
2	$\geq 10^{-3}$ to $<10^{-2}$	$>10^{2}$ to $\leq 10^{3}$	99% to 99.9%
1	$\geq 10^{-2}$ to $<10^{-1}$	>10 to $\leq 10^{2}$	90 to 99%

*** Approximating 1 year = 10,000 hrs of operation**

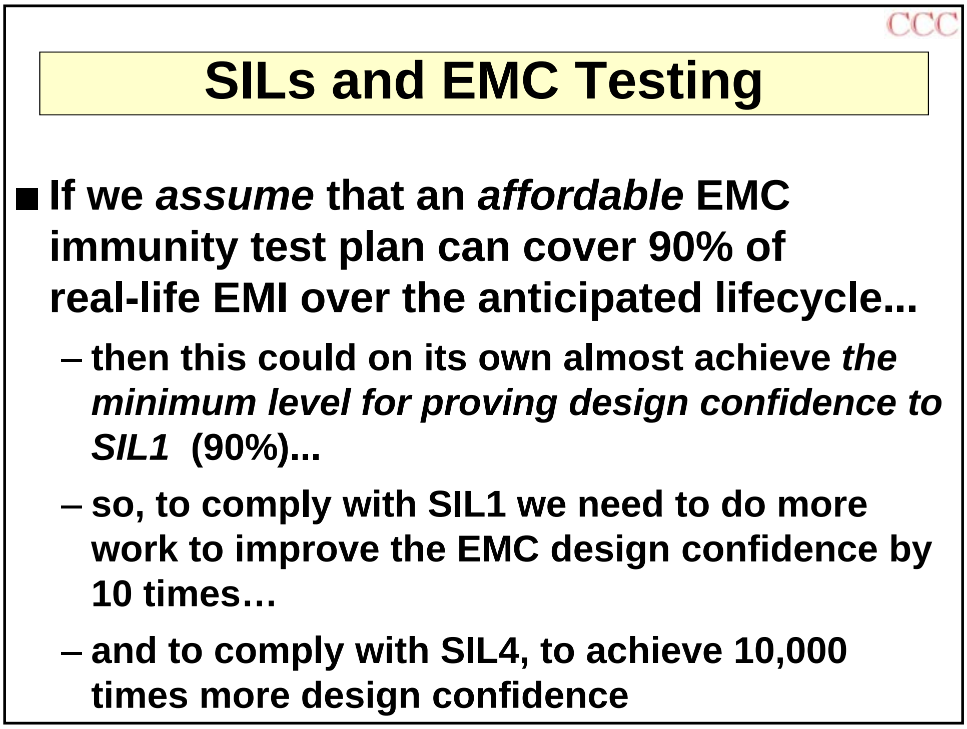
"Failure" includes any error, malfunction or fault that causes a hazard



SILs for "*continuous*" system functions...

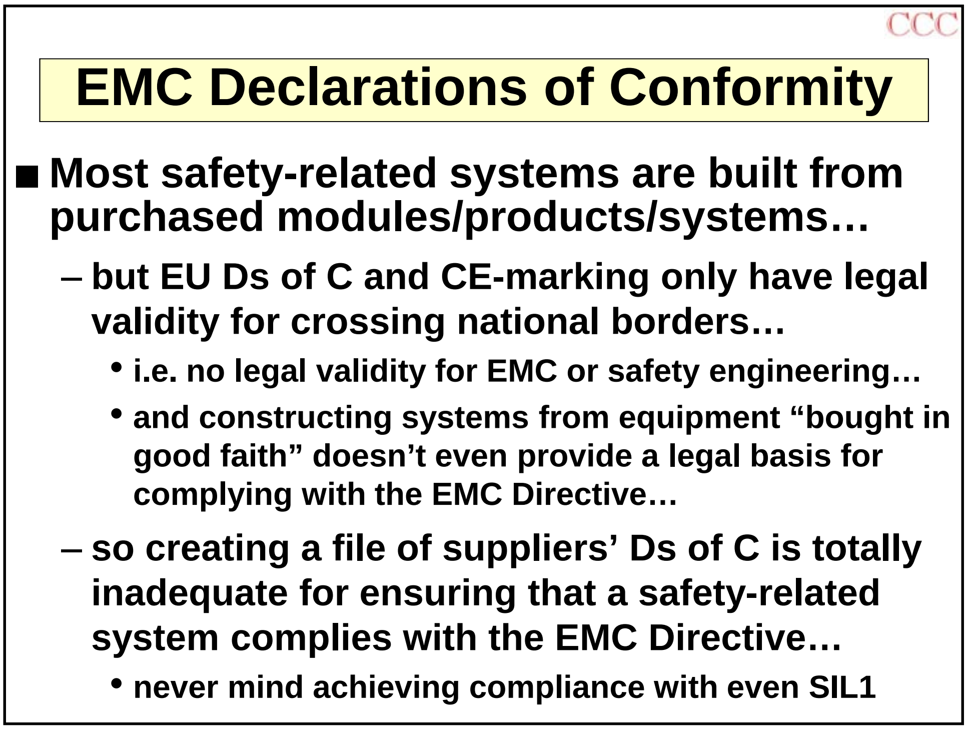
Safety Integrity Level (SIL)	Average probability of a dangerous failure per hour	Equivalent mean time to dangerous failure, in hours	Equivalent confidence factor required for every 10,000 hours of continuous operation
4	$\geq 10^{-9}$ to $<10^{-8}$	$>10^{8}$ to $\leq 10^{9}$	99.99 to 99.999%
3	$\geq 10^{-8}$ to $<10^{-7}$	$>10^{7}$ to $\leq 10^{8}$	99.9 to 99.99%
2	$\geq 10^{-7}$ to $<10^{-6}$	$>10^{6}$ to $\leq 10^{7}$	99% to 99.9%
1	$\geq 10^{-6}$ to $<10^{-5}$	$>10^{4}$ to $\leq 10^{5}$	90 to 99%

"Failure" includes any error, malfunction or fault that causes a hazard



SILs and EMC Testing

- If we *assume* that an *affordable* EMC immunity test plan can cover 90% of real-life EMI over the anticipated lifecycle...
  - then this could on its own almost achieve *the minimum level for proving design confidence to SIL1* (90%)...
  - so, to comply with SIL1 we need to do more work to improve the EMC design confidence by 10 times…
  - and to comply with SIL4, to achieve 10,000 times more design confidence



EMC Declarations of Conformity

- Most safety-related systems are built from purchased modules/products/systems…
  - but EU Ds of C and CE-marking only have legal validity for crossing national borders…
    - i.e. no legal validity for EMC or safety engineering…
    - and constructing systems from equipment “bought in good faith” doesn’t even provide a legal basis for complying with the EMC Directive…
  - so creating a file of suppliers’ Ds of C is totally inadequate for ensuring that a safety-related system complies with the EMC Directive…
    - never mind achieving compliance with even SIL1

Failures due to EMI are usually not identified

- People often say that normal EMC testing *must be* good enough for any risk level...
  - because we don't hear of failures caused by EMI
- But this is because EMI is hard to detect; usually leaves no trace, and is very difficult to duplicate...
  - and because most people aren't trained in EMI; accident inspectors ignore EMI, or treat it simplistically; and error-correction and watchdogs in modern products hide EMI effects

Failures due to EMI are usually not identified continued...

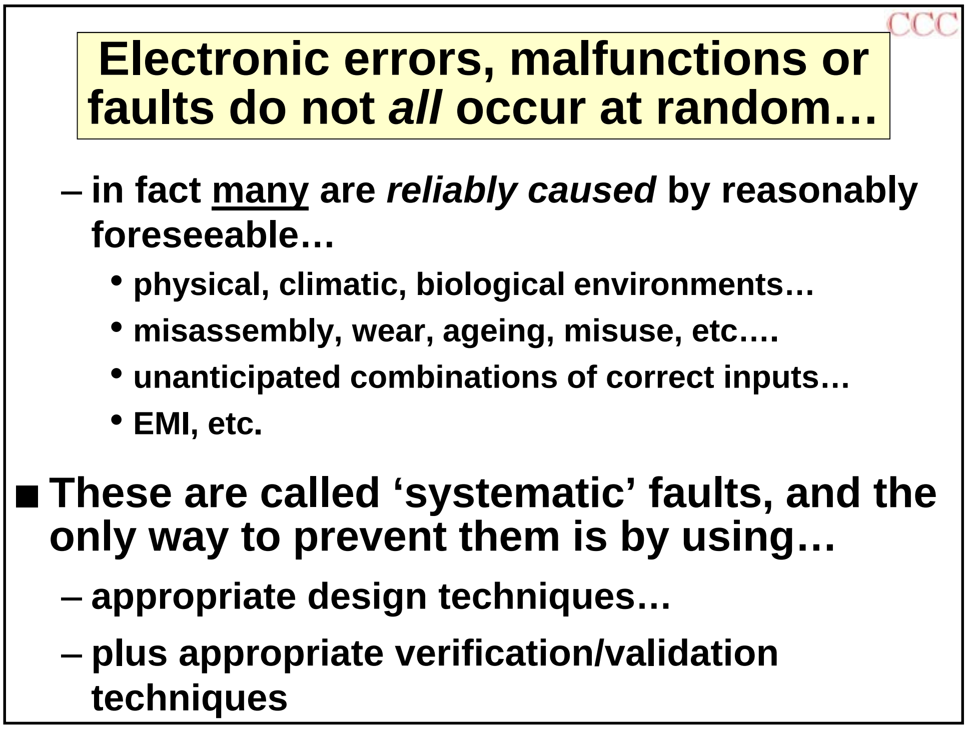
- It is sometimes said that the absence of evidence of EMI, is proof that EMI *can not* be a significant cause of failure...
  - but such types of arguments have been known to be logically defective since the 1800s...
    - yet are still used because they sound plausible to people who don't know better
- If a competent and comprehensive risk assessment shows there is a risk from EMI...
  - then (on average) the EMI failures ***will occur***, whether they are detected as such or not

Risk Assessment of EMI

- **The most powerful EMC design technique for Functional Safety…**
  - **is not to use any electronic technologies in the safety-related system !!!**
- **Electromechanical technologies (e.g. relays, contactors, solenoids, etc.) also have significant EMI problems…**
  - **which can often be avoided by adding cost (e.g. powering them from float-charged batteries)…**
  - **or not using them, either**

Some EMI issues important for EMC Risk Assessment

- **So-called “single-fault safety” is based on a faulty premise…**
  - **in fact, hazards can be caused by multiple *independent* errors, malfunctions and/or faults…**
  - **that can occur during the lifecycle**



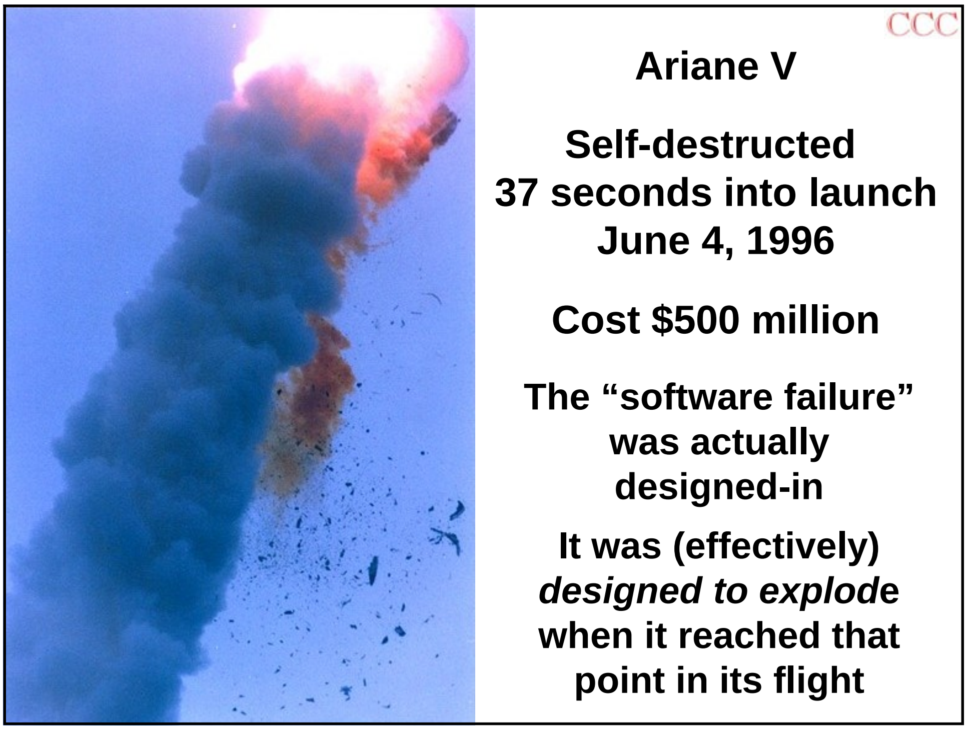
CCC

Electronic errors, malfunctions or faults do not *all* occur at random…

- in fact many are *reliably caused* by reasonably foreseeable…
  - physical, climatic, biological environments…
  - misassembly, wear, ageing, misuse, etc.…
  - unanticipated combinations of correct inputs…
  - EMI, etc.

■ These are called ‘systematic’ faults, and the only way to prevent them is by using…

- appropriate design techniques…
- plus appropriate verification/validation techniques



CCC

Ariane V

Self-destructed
37 seconds into launch
June 4, 1996

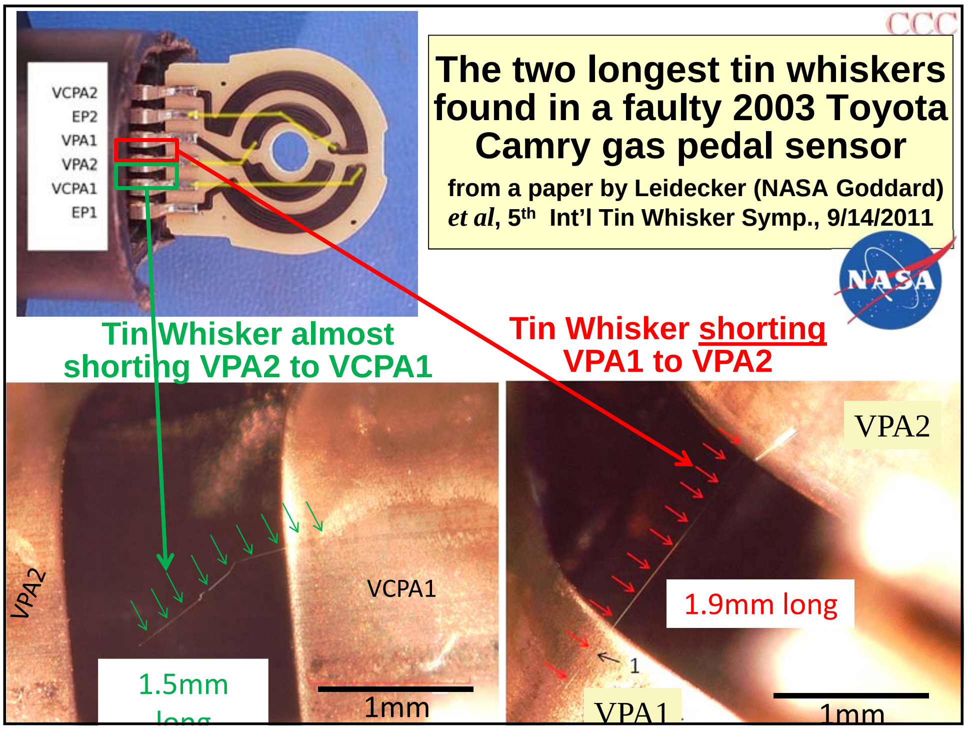
Cost $500 million

The “software failure” was actually designed-in

It was (effectively) *designed to explode* when it reached that point in its flight

Failures and faults are not *all* permanent

- In fact, many of them are temporary, e.g...
  - intermittent electrical connections…
    - in connectors, PCB-mounted components or their solder joints, etc…
  - transient EMI events...
  - errors or malfunctions corrected by communication protocols, error recovery/correction or automatic rebooting (e.g. by a watchdog timer), or even by manual power cycling

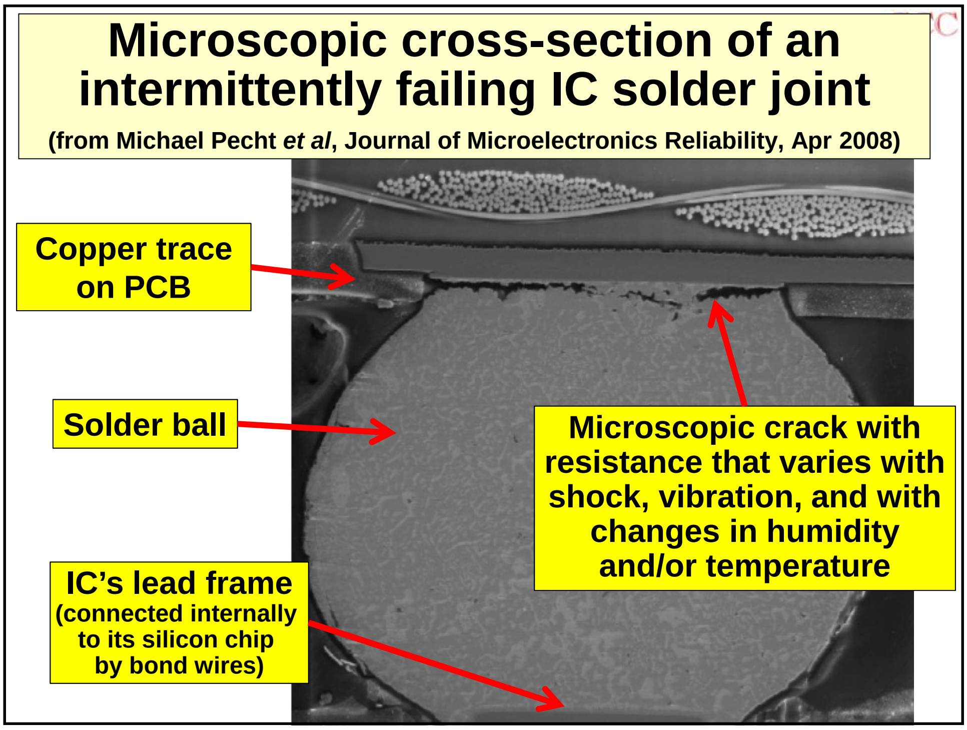


The two longest tin whiskers found in a faulty 2003 Toyota Camry gas pedal sensor

from a paper by Leidecker (NASA Goddard) *et al*, 5th Int'l Tin Whisker Symp., 9/14/2011

Tin Whisker almost shorting VPA2 to VCPA1

Tin Whisker <u>shorting</u> VPA1 to VPA2



Microscopic cross-section of an intermittently failing IC solder joint

(from Michael Pecht *et al*, Journal of Microelectronics Reliability, Apr 2008)

Copper trace on PCB

Solder ball

IC's lead frame (connected internally to its silicon chip by bond wires)

Microscopic crack with resistance that varies with shock, vibration, and with changes in humidity and/or temperature

Reducing risks with redundancy (i.e. using two or more parallel "channels")

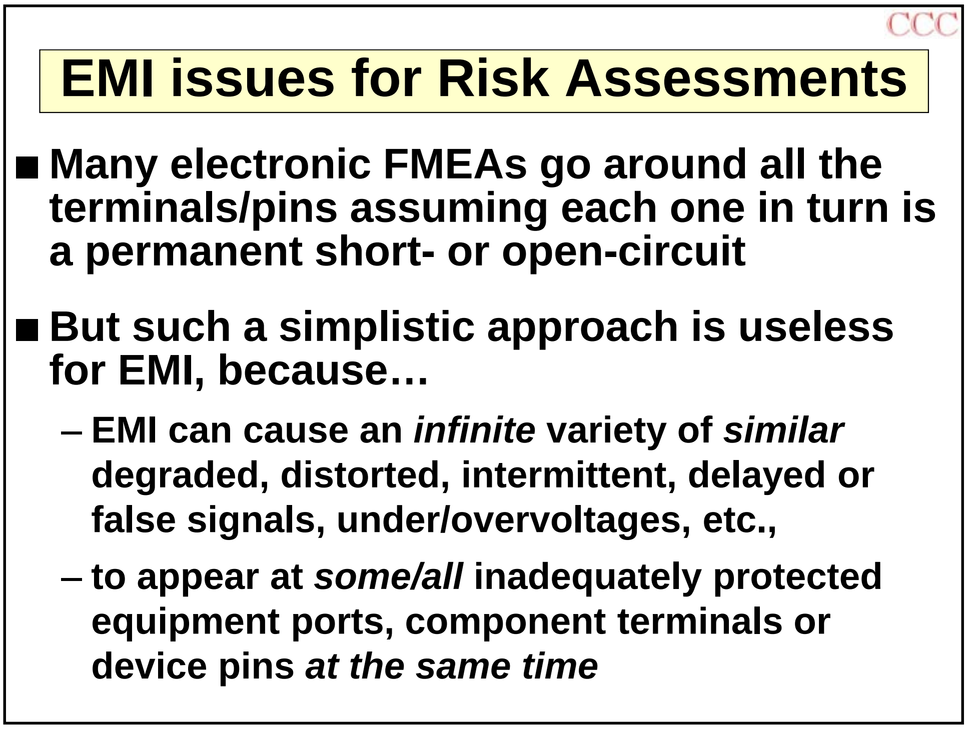
- When the channels use identical (or similar) hardware or software (e.g. to keep costs low)…
  - systematic errors, malfunctions or faults can affect both of them in the same way...
    - not necessarily at exactly the same time…
  - reducing/removing the risk reduction benefits of the multiple redundant channels
- This is called a "common-cause" error, malfunction or failure…
  - and is often caused by EMI

Reasonably foreseeable use or misuse is another important issue to take into account

- Never assume that someone would not do something because it would be 'too stupid'…
  - or that equipment is always operated by the correct people…
  - or that people always follow the User Manual or their manager's procedures and rules

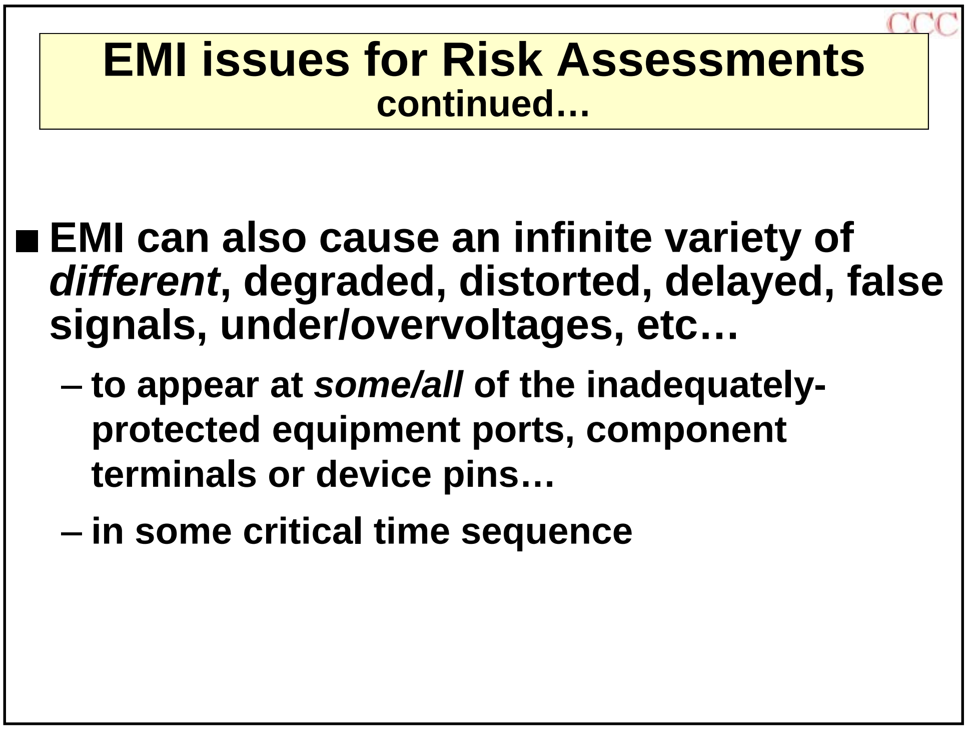
Risk Assessment of EMI continued...

- No standardised risk assessment methods have (yet) been developed for EMI…
  - so we have to choose which methods to use (FMEA, Fault Tree, SWIFT, etc.)…
  - Functional Safety experts recommend using *at least one* inductive method, plus *at least one* deductive method, plus *at least one* brainstorming method…
    - which we must competently adapt them to take all EMI possibilities into account...
    - at least including the EMI issues discussed in the following slides…



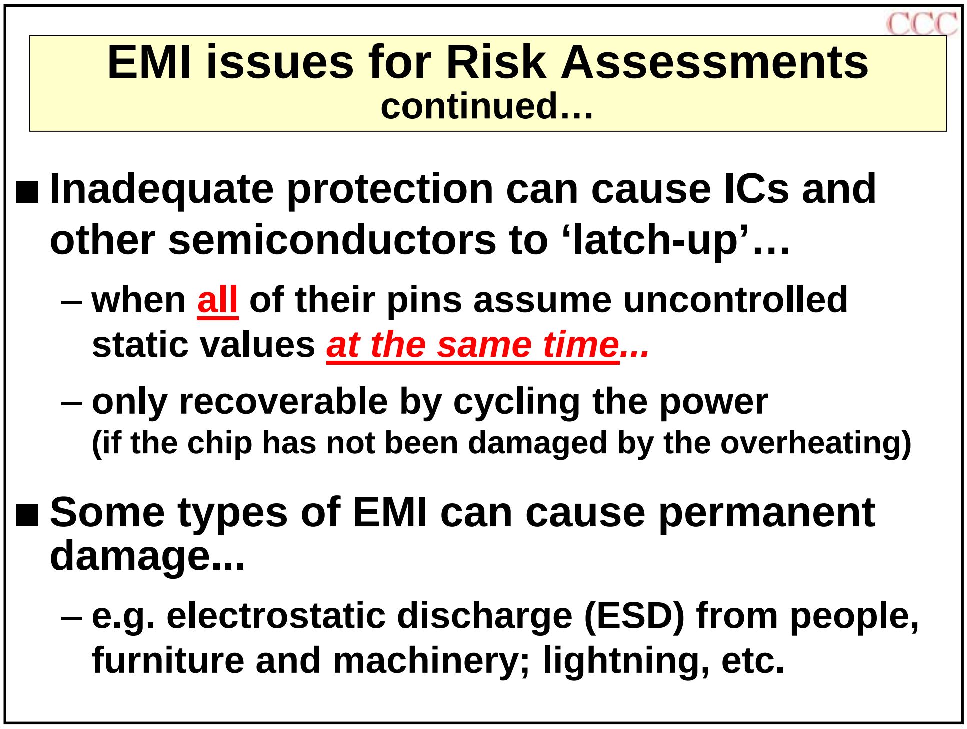
EMI issues for Risk Assessments

- Many electronic FMEAs go around all the terminals/pins assuming each one in turn is a permanent short- or open-circuit
- But such a simplistic approach is useless for EMI, because…
  - EMI can cause an *infinite* variety of *similar* degraded, distorted, intermittent, delayed or false signals, under/overvoltages, etc.,
  - to appear at *some/all* inadequately protected equipment ports, component terminals or device pins *at the same time*



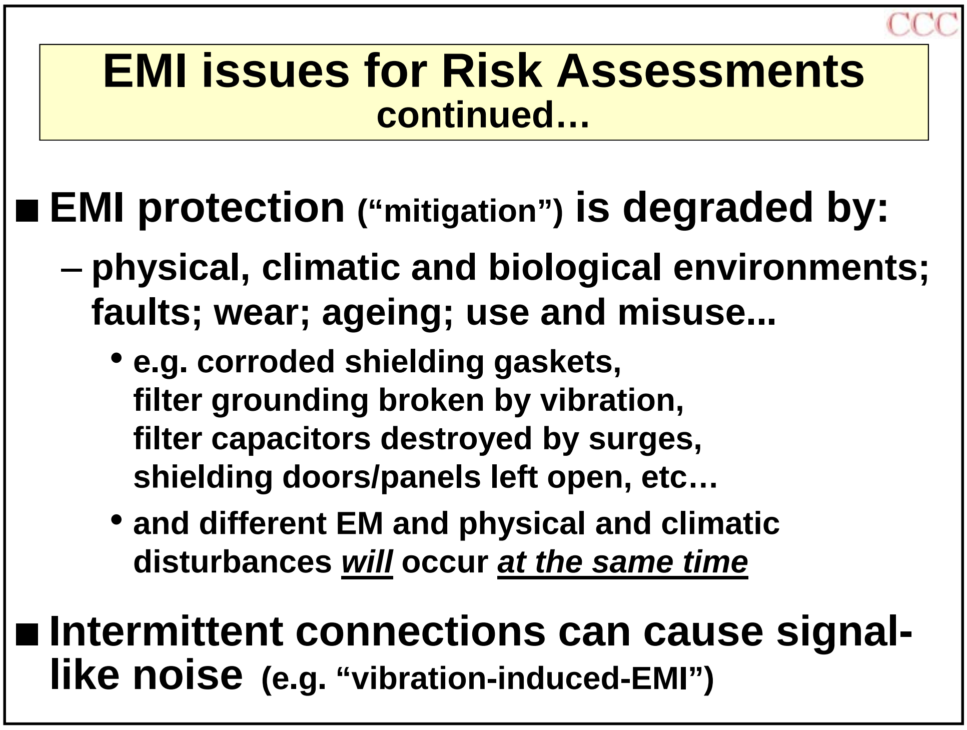
EMI issues for Risk Assessments continued…

- EMI can also cause an infinite variety of *different*, degraded, distorted, delayed, false signals, under/overvoltages, etc…
  - to appear at *some/all* of the inadequately-protected equipment ports, component terminals or device pins…
  - in some critical time sequence



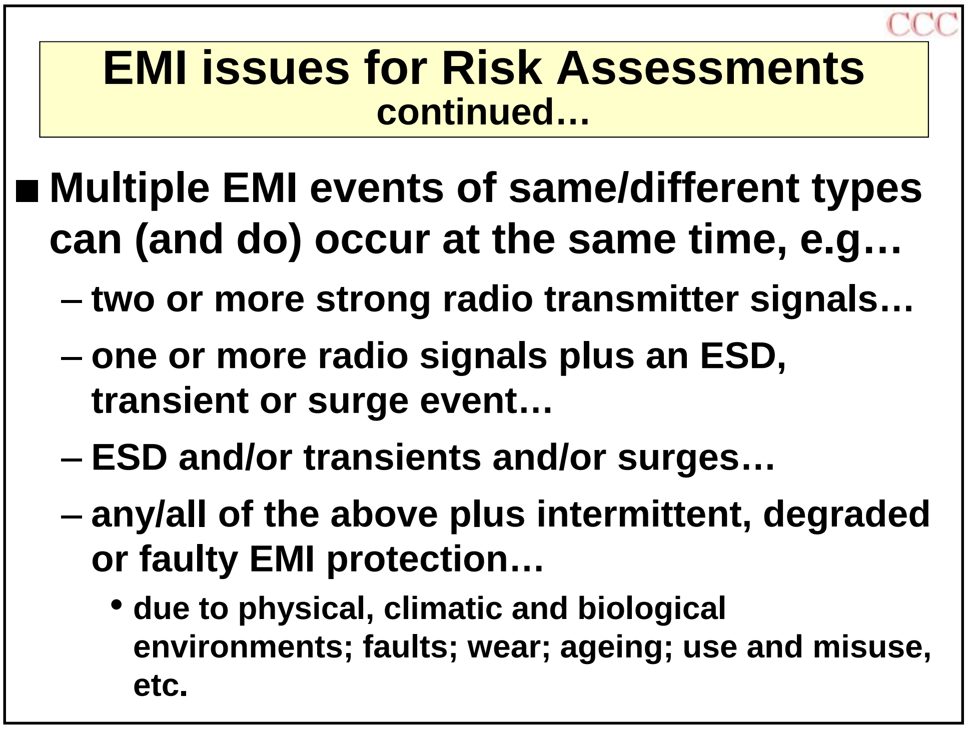
EMI issues for Risk Assessments
continued…

- Inadequate protection can cause ICs and other semiconductors to ‘latch-up’…
  - when all of their pins assume uncontrolled static values *at the same time*...
  - only recoverable by cycling the power (if the chip has not been damaged by the overheating)
- Some types of EMI can cause permanent damage...
  - e.g. electrostatic discharge (ESD) from people, furniture and machinery; lightning, etc.



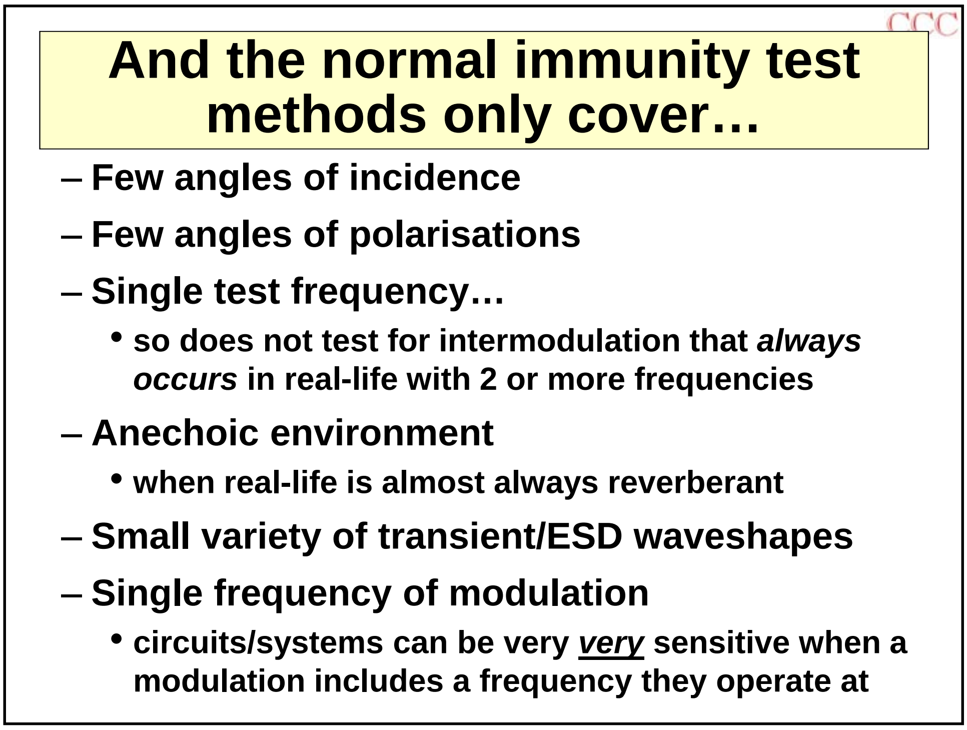
EMI issues for Risk Assessments
continued…

- EMI protection (“mitigation”) is degraded by:
  - physical, climatic and biological environments; faults; wear; ageing; use and misuse...
    - e.g. corroded shielding gaskets,
      filter grounding broken by vibration,
      filter capacitors destroyed by surges,
      shielding doors/panels left open, etc…
    - and different EM and physical and climatic disturbances *will* occur *at the same time*
- Intermittent connections can cause signal-like noise (e.g. “vibration-induced-EMI”)



EMI issues for Risk Assessments continued…

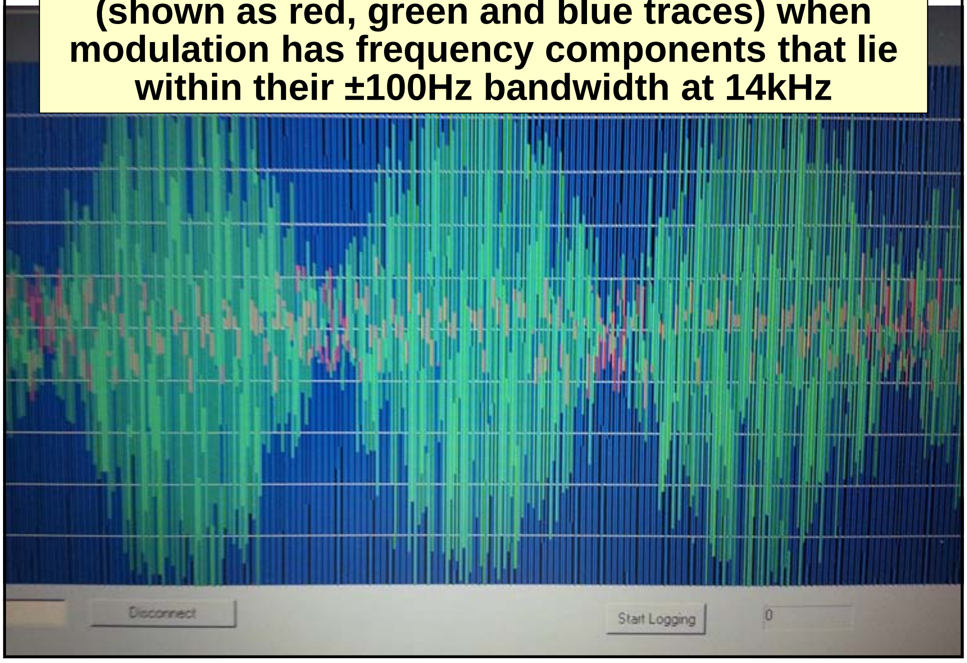
- Multiple EMI events of same/different types can (and do) occur at the same time, e.g…
  - two or more strong radio transmitter signals…
  - one or more radio signals plus an ESD, transient or surge event…
  - ESD and/or transients and/or surges…
  - any/all of the above plus intermittent, degraded or faulty EMI protection…
    - due to physical, climatic and biological environments; faults; wear; ageing; use and misuse, etc.



And the normal immunity test methods only cover…

- Few angles of incidence
- Few angles of polarisations
- Single test frequency…
  - so does not test for intermodulation that *always occurs* in real-life with 2 or more frequencies
- Anechoic environment
  - when real-life is almost always reverberant
- Small variety of transient/ESD waveshapes
- Single frequency of modulation
  - circuits/systems can be very *very* sensitive when a modulation includes a frequency they operate at

Full-scale noise on a 3-axis solid-state gyro (shown as red, green and blue traces) when modulation has frequency components that lie within their ±100Hz bandwidth at 14kHz



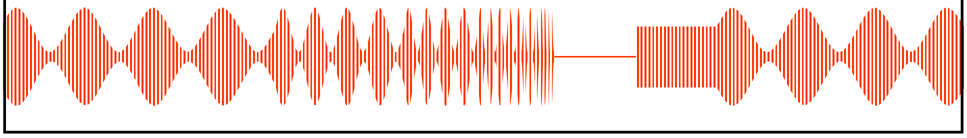
Design, and design assessment

- Dealing with all of the above seems almost impossible…
  - and ***it is impossible*** to create an immunity test plan that covers them all for SIL 2, 3 or 4…
  - that anyone – even National Governments – could afford, either in time or cost…
    - the exact same problem applies to software testing
- Immunity testing can be improved to get greater "fault coverage"…
  - e.g. by testing with two or more frequencies at the same time, to test intermodulation

CCC

Special modulation techniques

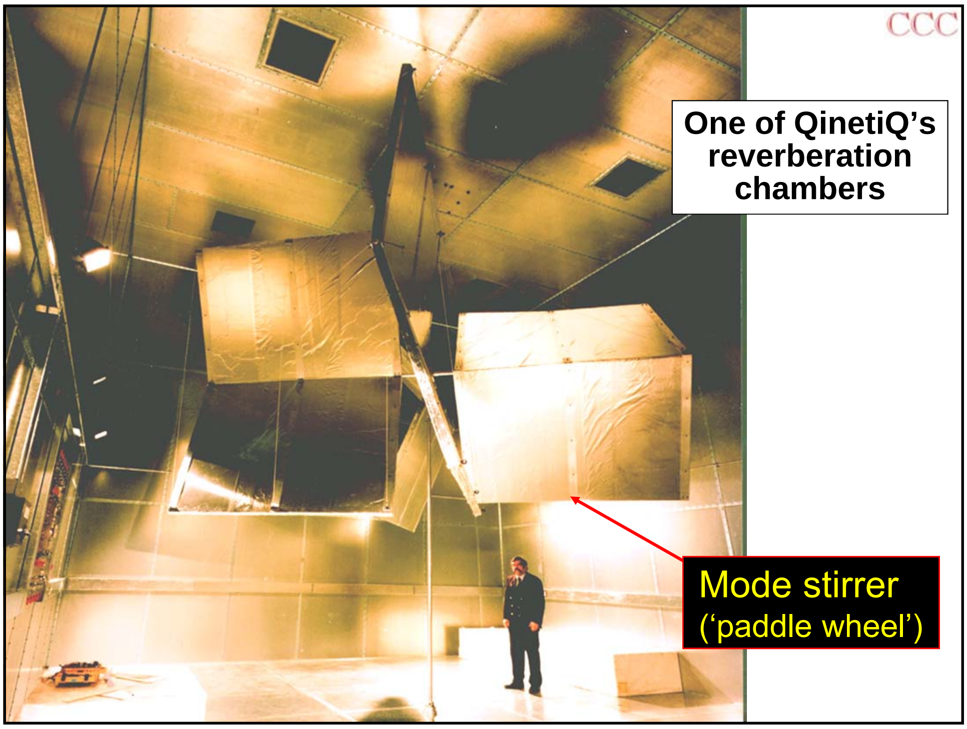
- Where especially susceptible frequencies or waveshapes are known, these are used as modulation during RF immunity tests…
    - recommended by MIL STD 461 and RTCA DO160
  - if not known, some EMC safety experts have developed special modulations, e.g.…
  - the radio field is ‘chirp modulated’ (e.g. from 10 Hz to 30 kHz), and also pulsed OFF for 1 s, then ON again (unmodulated) for 1 s…



CCC

Improved the coverage of radiated RF immunity tests

- Reverberation chamber (RC) tests are generally more realistic than anechoic chambers…
  - they cover all angles of incidence and polarisations with fewer tests…
  - and cost less…
  - and don’t need such powerful amplifiers
  - helping save time and cost compared with anechoic chamber testing



One of QinetiQ’s reverberation chambers

Mode stirrer (‘paddle wheel’)

Example of a radiated RF immunity test method currently employed on some safety systems

- **The reverb chamber’s stirrer rotates over a full revolution, in a series of steps**
  - **at each stirrer step, RF fields are generated covering the range of frequencies and magnitudes of the foreseeable real-life radiated EM threats**
  - **the frequency range is covered in small steps**
  - **and at each step the ‘chirp + pulsed Off/On’ or known susceptible frequencies/waveforms (see earlier) are emitted or used as modulation**

EMC design, and design assessment for *any* SIL

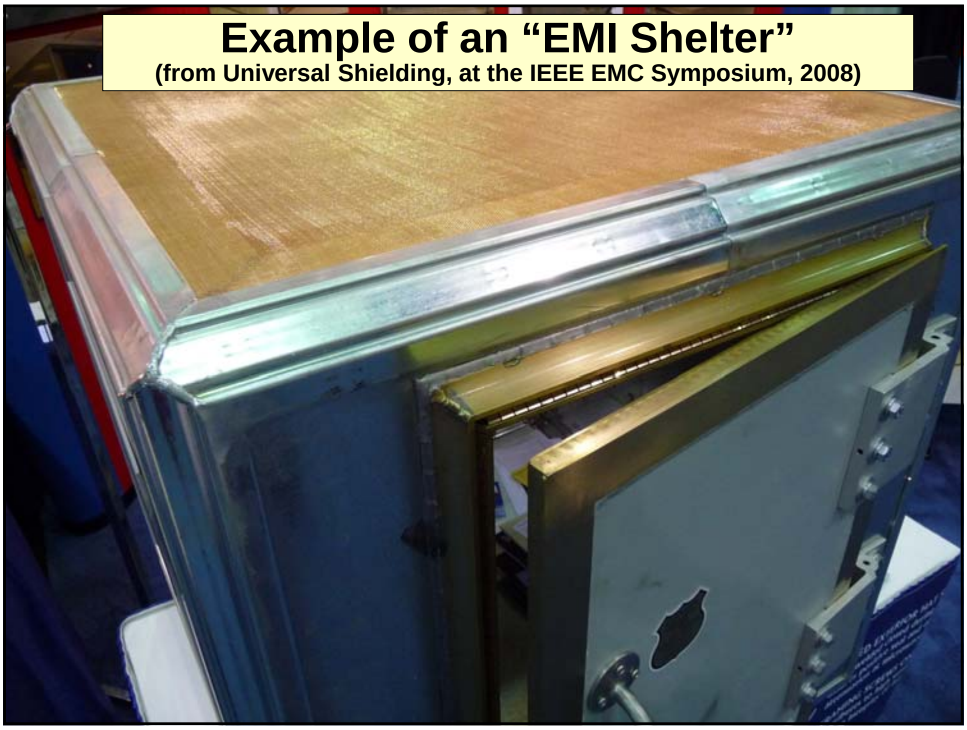
- Even with such testing improvements, it would be almost impossible to get beyond SIL 1
- There are two well-proven methods for achieving *any* SIL for all EMI issues…
  - the "EMI Shelter" approach…
  - the error detection/correction approach

The "EMI Shelter" approach…

  - is based on using a physically-rugged high-spec. shielded/filtered enclosure…
  - usually with fibre-optic datacommunications
- It is a "brute force" approach often used by the military, nuclear industry, etc…
  - but it is often too large, heavy, costly (or even just too ugly) for most other applications...
  - although fibre-optic datacomm's are *always* a good idea…
    - and are continually reducing in price

Example of an “EMI Shelter”

(from Universal Shielding, at the IEEE EMC Symposium, 2008)



The error detection/correction approach…

- uses hardware and software techniques that can be mathematically proven to detect and/or correct a certain % of the errors that can occur in signals, data, processing, and power rails…
- chosen to give a % “fault coverage” that is appropriate for the SIL

■ **On detection of an error…**

- either activate an alarm, switch the equipment into a safe state (if it has one)…
- or correct the errors so that normal (low-enough risk) operation continues

The error detection/correction approach continued…

- Uses techniques listed in 61508…
  - and so are very familiar to all functional safety designers, and their independent functional safety assessors
- Until now, there has been no guidance on using error correction/detection techniques for EMC (in 61508, 61000-1-2, the 2008 IET guide, etc.)…
  - but the IET Working Group is *right now* (Feb 2013) finalising suitable guidance…
  - which will be published in 2013 as an annex to the IET's 2008 Guide

Examples of error detection and correction techniques…

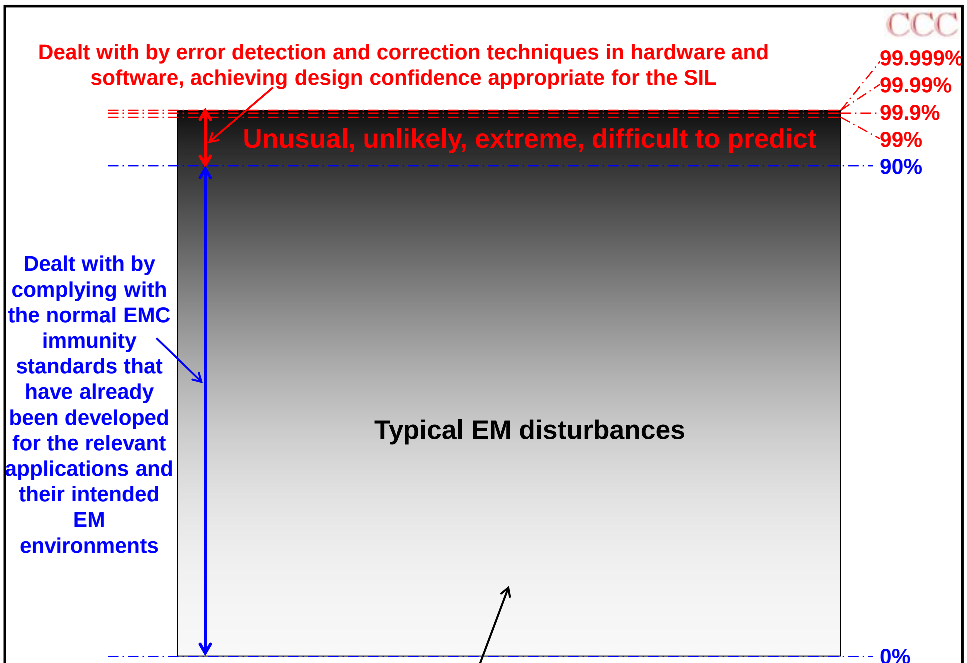
- Hardware built-in self-testing techniques, static and dynamic
- Data coding techniques, e.g. checksums, Hamming codes, CRC, etc.
- Plausibility techniques (e.g. measurements that appear to show a vessel is heating much more quickly than is possible given its mass and heater power, can be ignored as false data)
- Monitoring the correct operation of software and hardware processes…
  - and the quality of the DC power rails
- Many techniques for software coding

Examples of error detection and correction techniques… continued…

- Comparison techniques employing redundancy/replication…
  - one of a pair of duplicated data or processes should be inverted, to help prevent common-cause failures…
  - when using 3 or more "parallel channels" with voting (e.g. 2 out of 3, 3 out of 4, etc.) the channels should all be technologically diverse to avoid common-cause failures.
  - Note: common cause failures are typical of EMI, because it affects any identical channels the same way at the same time, making comparison methods ineffective. However many channels are used, common cause failure means the risks are the same as using just one channel.

The error detection/correction approach continued…

- Solely relying on error detection and "failing-safe", creates systems that suffer from too much downtime…
  - they are safe, but they don't work most of the time!
  - so when using this approach we also need compliance with *(at least)* the normal EMC immunity tests for the application and the EM environment(s)…
    - e.g. for compliance with the EMC Directive, or customer EMC specifications e.g. railway, automobile, military, power generation, etc.
  - so that "fail-safes" are not *too* common



Dealt with by error detection and correction techniques in hardware and software, achieving design confidence appropriate for the SIL

Unusual, unlikely, extreme, difficult to predict

Dealt with by complying with the normal EMC immunity standards that have already been developed for the relevant applications and their intended EM environments

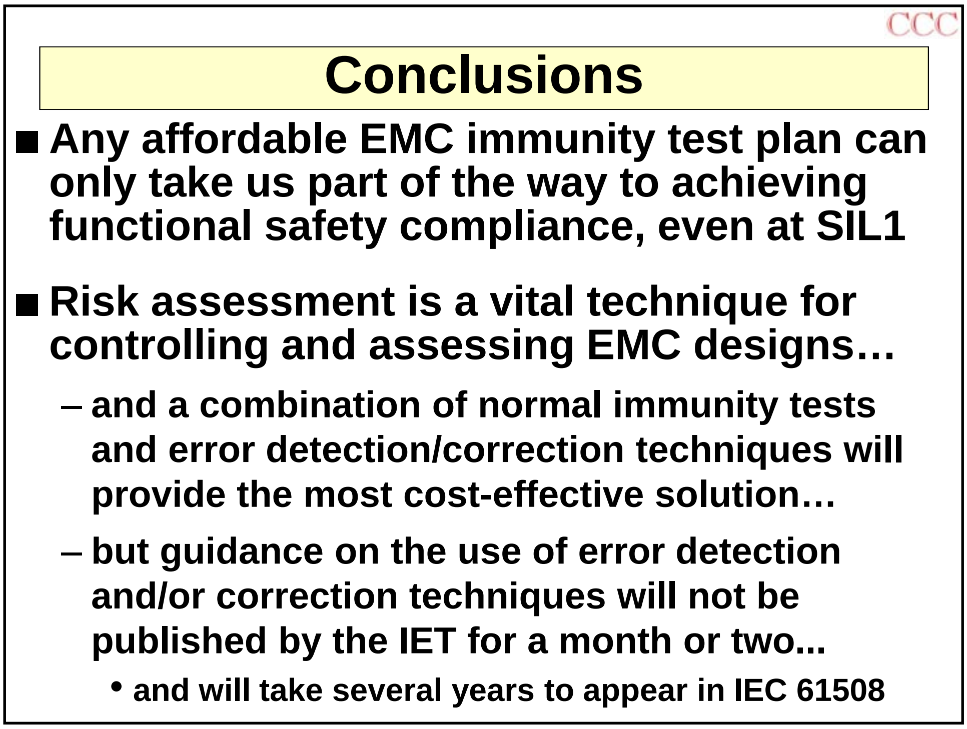
Typical EM disturbances

99.999%
99.99%
99.9%
99%
90%
0%

The total EM Environment over the lifetime of the equipment

The error detection/correction approach continued…

- Another reason for complying with (at least) the normal EMC immunity tests for the application and the EM environment, so that "fail-safes" are not *too* common…
  - is that operators/users/owners are likely to modify the safety systems to improve uptime…
    - without the approval of the manufacturer…
  - causing unsafe systems...
  - but this would be *the manufacturer's fault* because he should have realised this would happen



Conclusions

- Any affordable EMC immunity test plan can only take us part of the way to achieving functional safety compliance, even at SIL1
- Risk assessment is a vital technique for controlling and assessing EMC designs…
  - and a combination of normal immunity tests and error detection/correction techniques will provide the most cost-effective solution…
  - but guidance on the use of error detection and/or correction techniques will not be published by the IET for a month or two...
    - and will take several years to appear in IEC 61508

KHBO Seminar, February 6, 2013

EMC for Functional Safety

the end

Keith Armstrong

www.cherryclough.com

Some quotations on EMI and EMI testing continued...

"…there is no way by testing to duplicate all the possible combinations of frequencies, amplitudes, modulation waveforms, spatial distributions, and relative timing of the many simultaneous interfering signals that an operating system may encounter.
As a result, it's going to fail."

from: "EMC Failures Happen", Ron Brewer, NARTE Certified EMC Engineer, IEEE EMC Society Distinguished Lecturer; in Evaluation Engineering magazine, Dec. 2007, www.evaluationengineering.com/features/2007_december/1207_emc_test.aspx

Some quotations on EMI and EMI testing continued...

"Although electronic components must pass a set of EMC tests to (help) ensure safe operations, the evolution of EMC over time is not characterized and cannot be accurately forecast."

from: Alexandre Boyer *et al*, "Characterization of the Evolution of IC Emissions After Accelerated Aging", IEEE Transactions on EMC, Vol. 51, No. 4, November 2009, pages 892-900

CCC

Some quotations on EMI and EMI testing continued...

"As indicated in [2] narrow-band threat fields with simple modulations are no longer necessarily representative of the EMI which causes the failure in digital systems."

from: "Preliminary Investigation into a Methodology for Assessing the Direct RF Susceptibility of Digital Hardware, Final Report for Radiocommunications Agency, Document No. R/99/042, Project No. 0921", Dr I D Flintoff, May 1999, www.ofcom.org/uk/static/archive/ra/topics/research/topics/emc/r99042/r99042.pdf

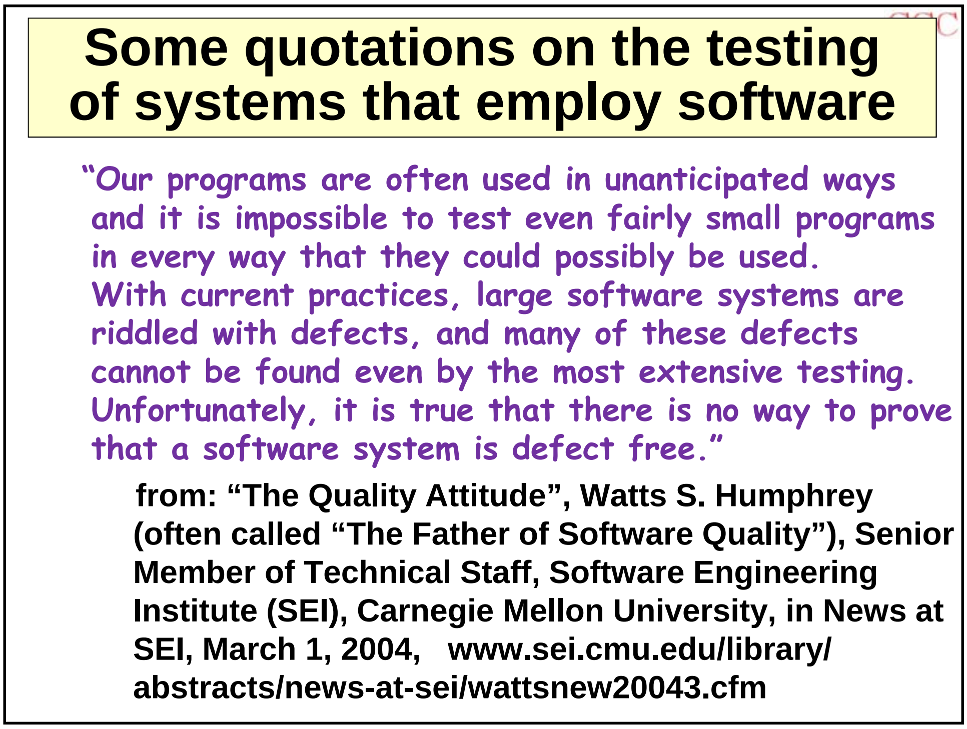
CCC

Some quotations on EMI and EMI testing continued...

"In most cases there is no simple or practicable way to check and to verify by means of testing or measuring that immunity is achieved for the safety-related system in its entirety with respect to other systems, equipment or the external electromagnetic environment for all operating conditions and operating modes."

"This is due to the fact that not every combination of operating conditions, of operating modes and of electromagnetic phenomena acting on the system can be achieved in a reasonable way and in a reasonable period."

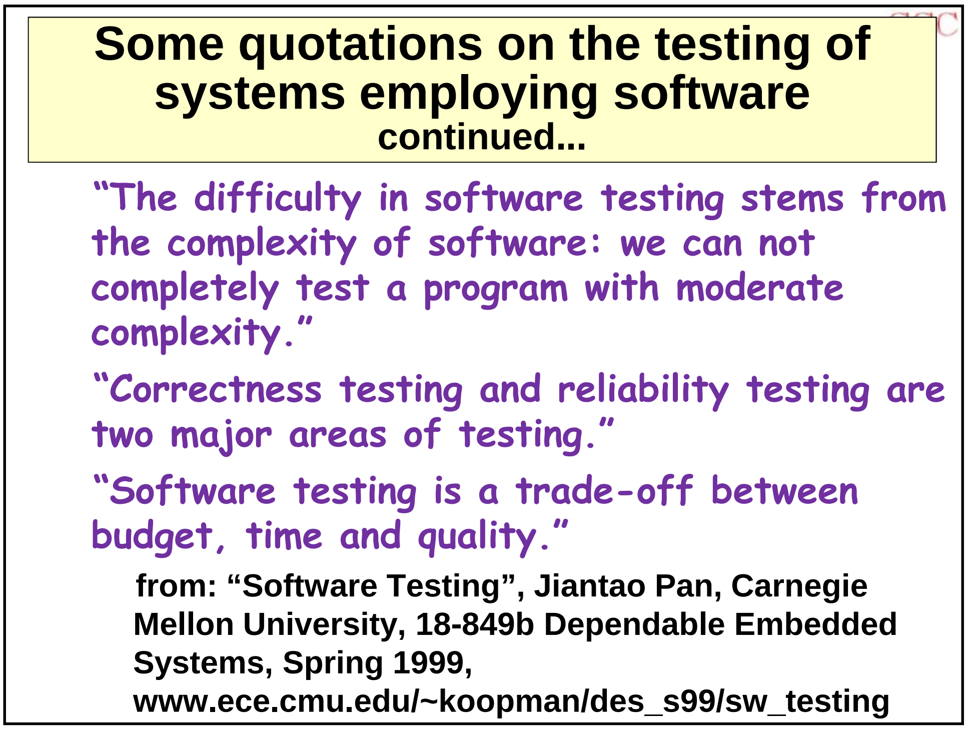
from: IEC TS 61000-1-2, Ed.2, December 2008



Some quotations on the testing of systems that employ software

"Our programs are often used in unanticipated ways and it is impossible to test even fairly small programs in every way that they could possibly be used. With current practices, large software systems are riddled with defects, and many of these defects cannot be found even by the most extensive testing. Unfortunately, it is true that there is no way to prove that a software system is defect free."

from: "The Quality Attitude", Watts S. Humphrey (often called "The Father of Software Quality"), Senior Member of Technical Staff, Software Engineering Institute (SEI), Carnegie Mellon University, in News at SEI, March 1, 2004, www.sei.cmu.edu/library/ abstracts/news-at-sei/wattsnew20043.cfm



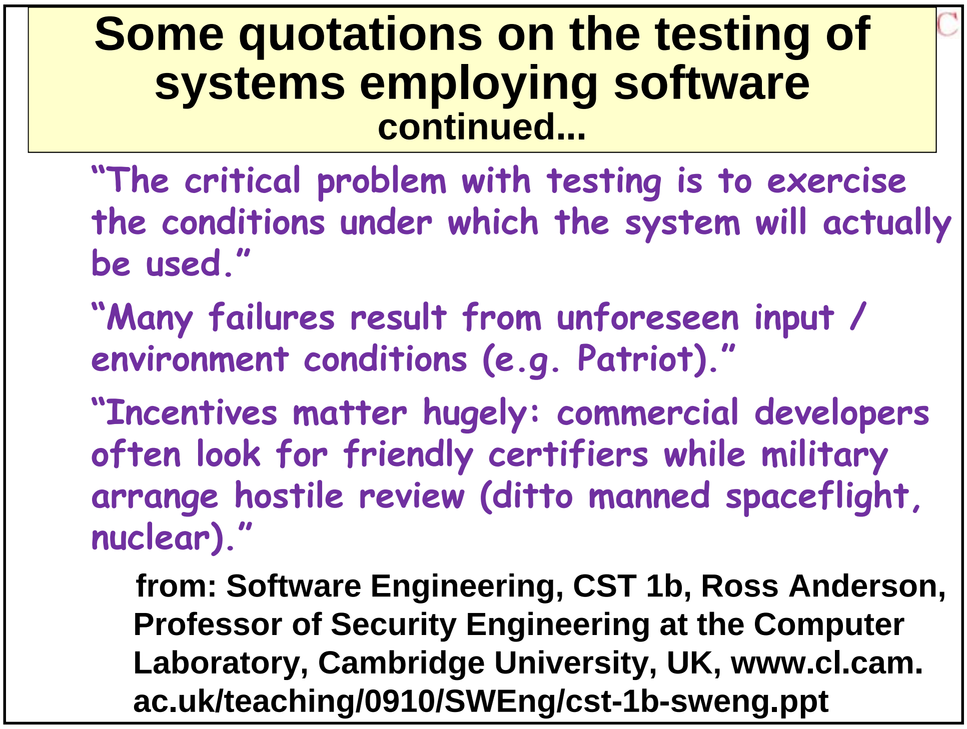
Some quotations on the testing of systems employing software continued...

"The difficulty in software testing stems from the complexity of software: we can not completely test a program with moderate complexity."

"Correctness testing and reliability testing are two major areas of testing."

"Software testing is a trade-off between budget, time and quality."

from: "Software Testing", Jiantao Pan, Carnegie Mellon University, 18-849b Dependable Embedded Systems, Spring 1999, www.ece.cmu.edu/~koopman/des_s99/sw_testing



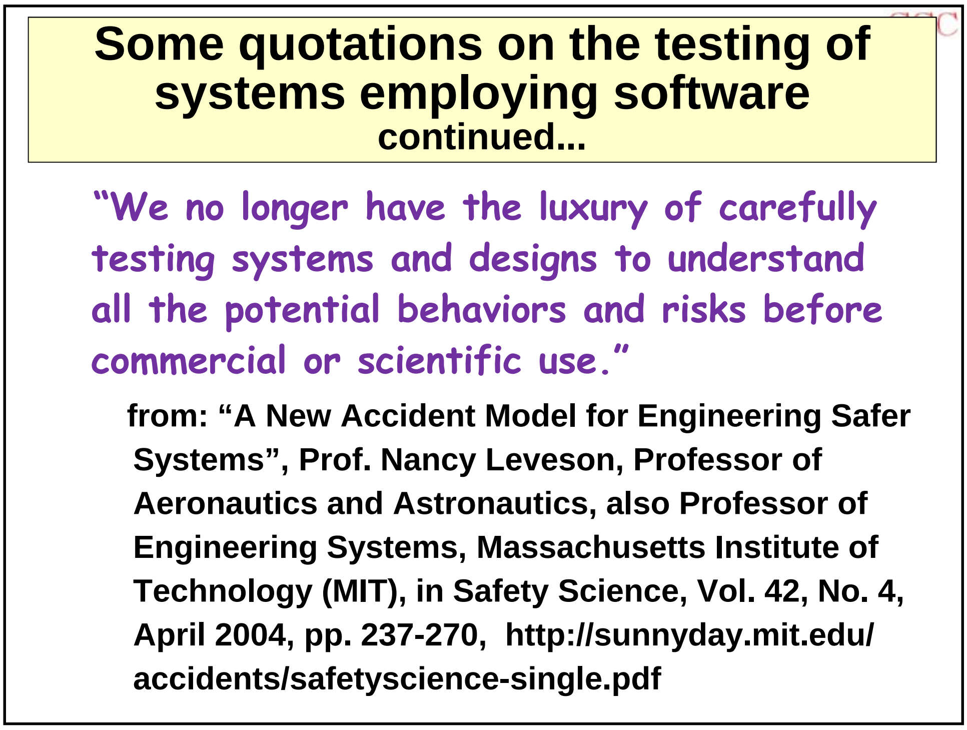
Some quotations on the testing of systems employing software continued...

"The critical problem with testing is to exercise the conditions under which the system will actually be used."

"Many failures result from unforeseen input / environment conditions (e.g. Patriot)."

"Incentives matter hugely: commercial developers often look for friendly certifiers while military arrange hostile review (ditto manned spaceflight, nuclear)."

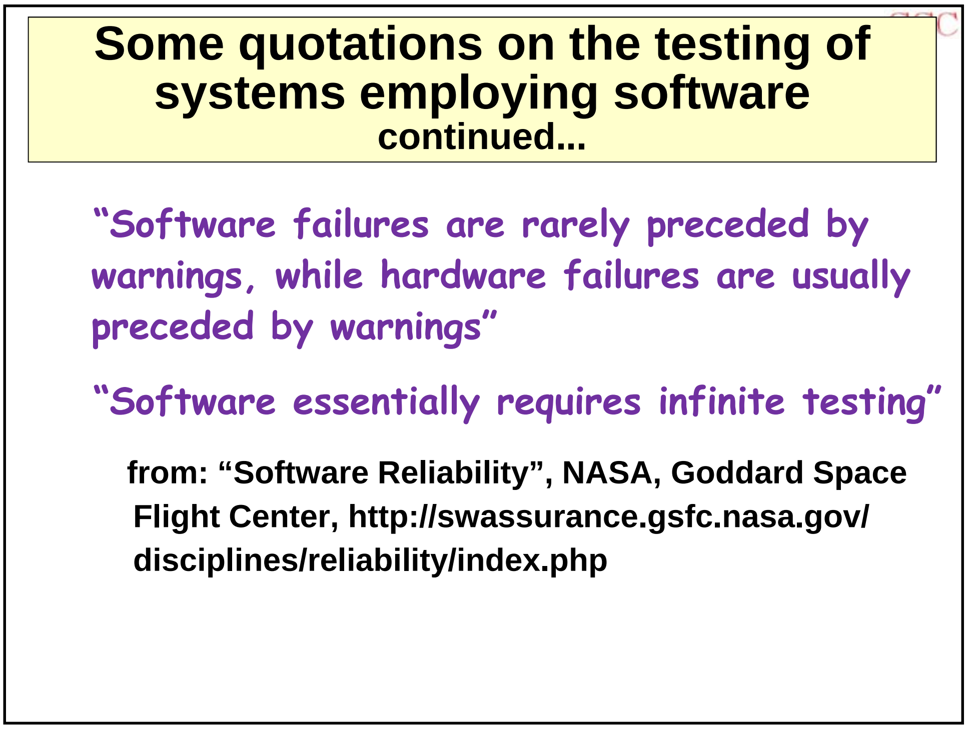
from: Software Engineering, CST 1b, Ross Anderson, Professor of Security Engineering at the Computer Laboratory, Cambridge University, UK, www.cl.cam.ac.uk/teaching/0910/SWEng/cst-1b-sweng.ppt



Some quotations on the testing of systems employing software continued...

"We no longer have the luxury of carefully testing systems and designs to understand all the potential behaviors and risks before commercial or scientific use."

from: "A New Accident Model for Engineering Safer Systems", Prof. Nancy Leveson, Professor of Aeronautics and Astronautics, also Professor of Engineering Systems, Massachusetts Institute of Technology (MIT), in Safety Science, Vol. 42, No. 4, April 2004, pp. 237-270, http://sunnyday.mit.edu/accidents/safetyscience-single.pdf

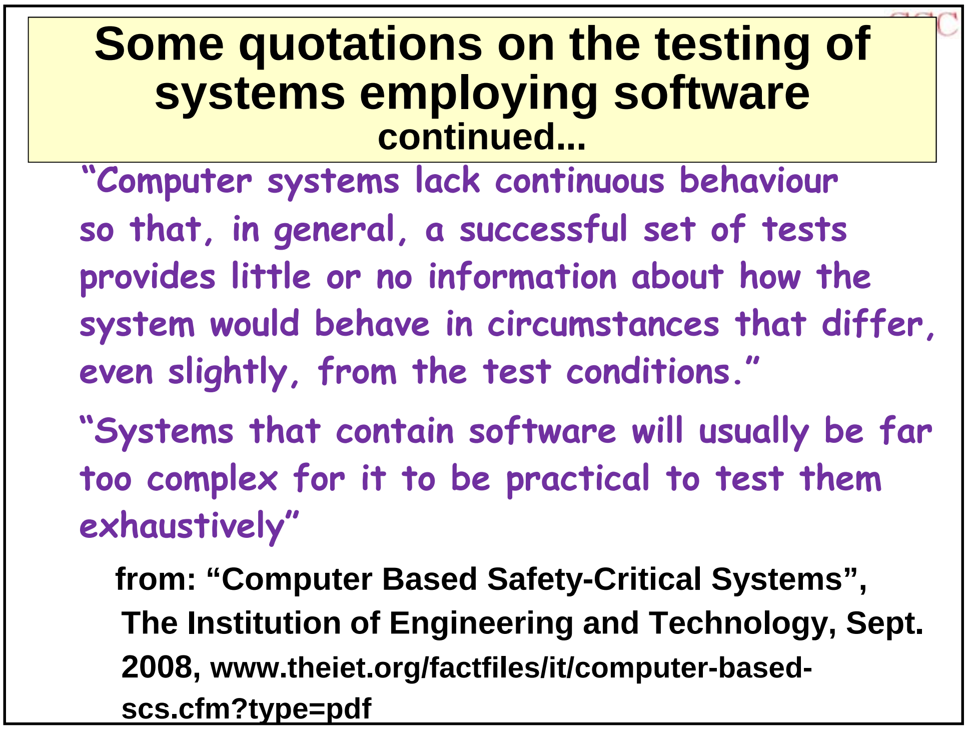


Some quotations on the testing of systems employing software continued...

"Software failures are rarely preceded by warnings, while hardware failures are usually preceded by warnings"

"Software essentially requires infinite testing"

from: "Software Reliability", NASA, Goddard Space Flight Center, http://swassurance.gsfc.nasa.gov/disciplines/reliability/index.php



Some quotations on the testing of systems employing software continued...

"Computer systems lack continuous behaviour so that, in general, a successful set of tests provides little or no information about how the system would behave in circumstances that differ, even slightly, from the test conditions."

"Systems that contain software will usually be far too complex for it to be practical to test them exhaustively"

from: "Computer Based Safety-Critical Systems", The Institution of Engineering and Technology, Sept. 2008, www.theiet.org/factfiles/it/computer-based-scs.cfm?type=pdf

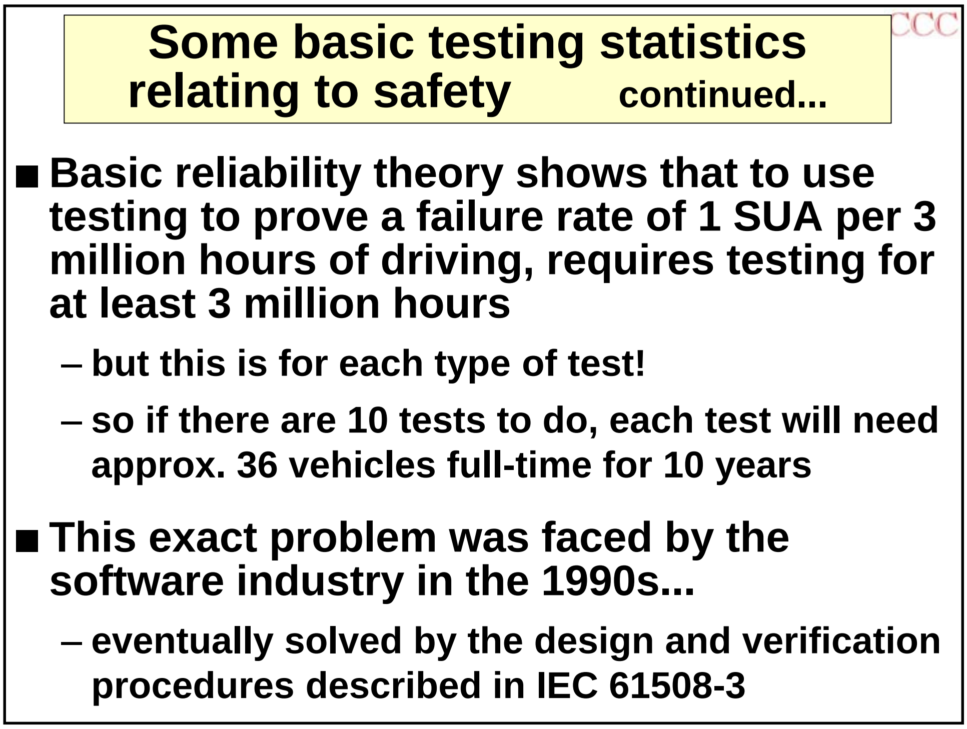
Some quotations on the testing of systems employing software
continued...

"It is generally impractical to rely on test-based evidence in advance of putting a system into widespread service that the overall probability will be less than 10^{-5} per hour with 99% confidence, equivalent to a mean time between failures of approximately one year."

from: "Computer Based Safety-Critical Systems", The Institution of Engineering and Technology, Sept. 2008, www.theiet.org/factfiles/it/computer-based-scs.cfm?type=pdf

A quick look at some basic testing statistics relating to safety

- **For example: NHTSA has had up to 3,000 complaints of Sudden Unintended Acceleration (SUA) in one year (1989-90)...**
  - **assuming 30 million vehicles on the road, that's a rate of 1 in 10,000 per vehicle per year...**
  - **assuming an average drive of 1 hr/day, 6 days/week, gives us one SA per 3,120,000 hours of driving...**
  - **to detect one SA in just one model would require testing 36 vehicles, 24/7, for 10 years!**
  - **or driving a single vehicle 200 million miles!**



Some basic testing statistics relating to safety continued...

- Basic reliability theory shows that to use testing to prove a failure rate of 1 SUA per 3 million hours of driving, requires testing for at least 3 million hours
  - but this is for each type of test!
  - so if there are 10 tests to do, each test will need approx. 36 vehicles full-time for 10 years
- This exact problem was faced by the software industry in the 1990s...
  - eventually solved by the design and verification procedures described in IEC 61508-3