Another EMC resource
from EMC Standards

Managing functional safety risks caused by EMI needs more than immunity testing IEEE Dresden 2015

Helping you solve your EMC problems

1 Brassey Road, Old Potts Way, Shrewsbury, SY3 7FA T:+44 (0) 1785 660 247 E:info@emcstandards.co.uk

CCC

Managing functional safety (and other) risks caused by EMI needs much more than immunity testing

An introduction to the IET's 2013 guidance on "EMI Resilience"

Keith Armstrong, C.Eng., FIET, Senior MIEEE, ACGI

CHERRY CLOUGH CONSULTANTS LTD

www.cherryclough.com

1 of 47

CCC

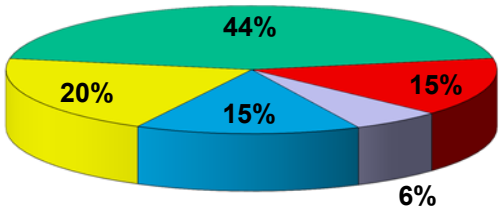
What is 'Functional Safety'?

- **The safety engineering discipline of Functional Safety is relatively new…**
  - **based upon IEC 61508, first published 2000, which defines it as…**
    - **"The part of the overall safety that depends on the correct functioning of the Electrical/Electronic/ Programmable Electronic (E/E/PE) safety-related systems and other risk reduction measures"**
  - **in other words…**
    - **Functional Safety is concerned with safety risks caused by errors, malfunctions and faults in the operation of hardware and software (inc. 'firmware')**

2 of 47

CCC

Most actual safety failures are *built-in*
(data from HSE investigations into major industrial accidents)



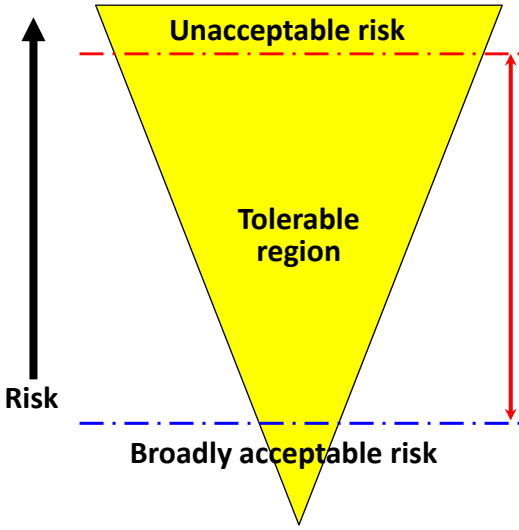
- Specification: 44%
- Design, implementation: 15%
- Installation, commissioning: 6%
- Operation, maintenance: 15%
- Changes after commissioning: 20%

> 60% of all failures are *built-in*

3 of 47

CCC

Acceptable levels of risk of death, per person, per year
(the HSE's "carrot diagram", 2001)



Probability of death: 10^{-3} (worker), 10^{-4} (public)

In this region, reduce risk until cost of further reduction is grossly disproportionate (10x) the value of the lives saved

Probability of death: 10^{-6} (all)
1 in a million, per person per year

4 of 47

CCC

Testing digital systems for Functional Safety is impossible

- A great many safety risks now depend on the correct functioning of electronics…
  - but for >30 years, it has been impossible to fully test a microprocessor…
  - or a software program of any size (Microsoft can only now fully test a Printer Driver)…
    - 100% testing a digital system needs millions of years!
- Digital systems are nonlinear…
  - so testing even 99% (say) of their digital states proves nothing about the safety of the 1% left...
    - so testing cannot prove safety, even at the 10^{-3} level

5 of 47

CCC

The solution: well-proven design "Techniques & Measures" (T&Ms)

- Because electronics cannot be proven safe-enough solely by testing…
  - a great deal of work has been done on proving T&Ms for design (Spec's, Systems, Hardware, Software)…
  - and T&Ms for verifying/validating designs
- These aim to ensure that any *possible* errors, malfunctions or faults in signals, data, control and power supplies are detected…
  - and either corrected so that operation continues safely-enough (perhaps with functional degradation)…
  - or the equipment switched to a "safe state"

6 of 47

CCC

"Techniques & Measures" (T&Ms)

- This massive work on T&Ms for functional safety originally published as IEC 61508:2000…
  - the "basic standard on Functional Safety"
- Depending on the amount of risk-reduction required to achieve acceptable safety level…
  - appropriate ranges of T&Ms are applied to each "safety-related system"…
  - plus appropriate levels of independent 3rd-Party design assessment…
  - to ensure sufficient *Design Confidence* in achieving Functional Safety

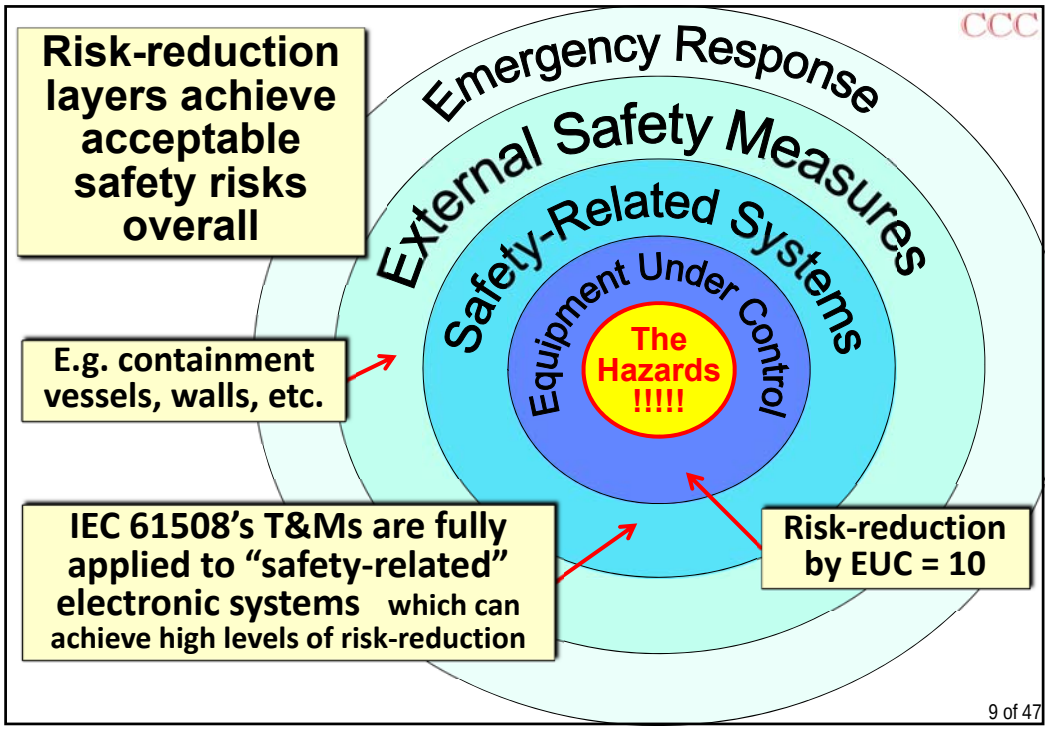
7 of 47

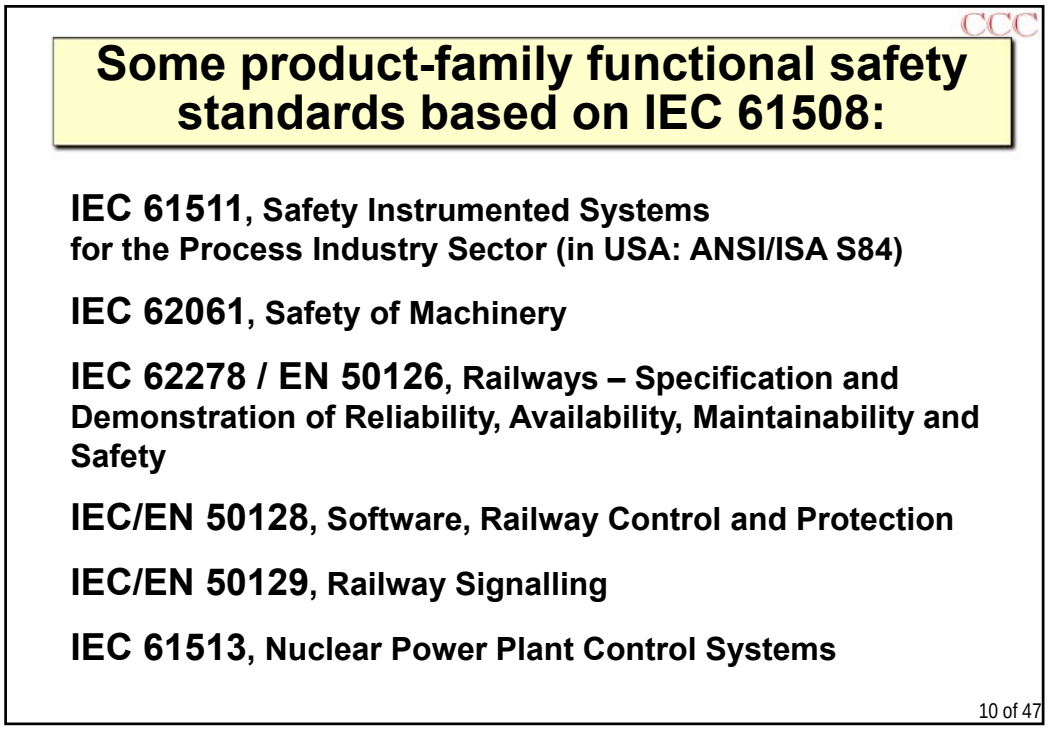
CCC

Achieving acceptable levels of safety risk

- The overall amount of risk-reduction needed to ensure acceptable safety risks…
  - relies on several nested 'layers' of risk reduction (see next slide)…
  - but IEC 61508's T&Ms are only relevant for the "safety-related" electronic systems
- Where the hazardous "equipment under control" (EUC) is too complex for 61508's T&Ms to be applied to it (e.g. a large process plant)…
  - using good engineering practices throughout the EUC is assumed to reduce the hazard's risks by 10

8 of 47


CCC
Risk-reduction layers achieve acceptable safety risks overall
Emergency Response
External Safety Measures
Safety-Related Systems
Equipment Under Control
The Hazards !!!!!
E.g. containment vessels, walls, etc.
IEC 61508's T&Ms are fully applied to "safety-related" electronic systems which can achieve high levels of risk-reduction
Risk-reduction by EUC = 10
9 of 47


CCC
Some product-family functional safety standards based on IEC 61508:
IEC 61511, Safety Instrumented Systems for the Process Industry Sector (in USA: ANSI/ISA S84)
IEC 62061, Safety of Machinery
IEC 62278 / EN 50126, Railways – Specification and Demonstration of Reliability, Availability, Maintainability and Safety
IEC/EN 50128, Software, Railway Control and Protection
IEC/EN 50129, Railway Signalling
IEC 61513, Nuclear Power Plant Control Systems
10 of 47

CCC

Some product-family functional safety standards based on IEC 61508 continued…

RTCA DO-178B, North American Avionics Software

RTCA DO-254, North American Avionics Hardware

EUROCAE ED-12B, European Flight Safety Systems

ISO 26262, Automobile Functional Safety

IEC 62304, Medical Device Software

IEC/EN 50402, Fixed Gas Detection Systems

DEF STAN 00-56, Accident Consequence (UK military)

Medical industry risk management standards use ISO 14971 instead of IEC 61508, but principles are same

11 of 47

CCC

The relationship between EMC and Functional Safety

- **Electromagnetic Interference (EMI) is a cause of errors, malfunctions and failures in *all* electronic technologies...**
  - **so *must* be taken into account when managing the functional safety risks caused by errors, malfunctions or faults in hardware or software**
- **but the Functional Safety engineering discipline shares *nothing* with EMC…**
  - **making communications between EMC engineers and Functional Safety engineers *very difficult indeed***

12 of 47

EMC testing is insufficient for Functional Safety

CCC

- We saw that it is impossible to test even 10% of the possible states of a digital system…
  - so it is ***even more impossible*** to test their immunity to a variety of EM disturbances
- But functional safety must be maintained over *the complete lifecycle* despite all foreseeable…
  - tolerances; assembly errors; faults; aging; wear; unusual, extreme & simultaneous EM disturbances; misuse; physical & climatic environments; etc., etc.
- So *no possible* EMC test plan could *possibly* provide enough EMC ***design confidence***

13 of 47

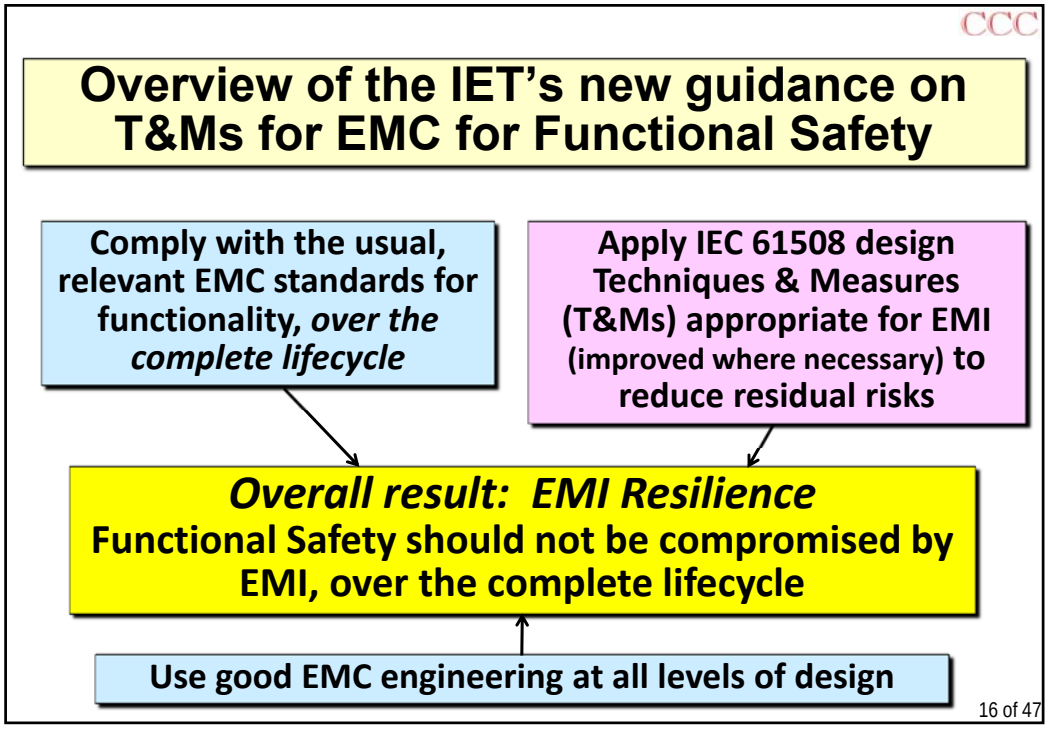
The traditional way of achieving functional safety despite an unknown EM environment…

CCC

- …is to use over-specified and ruggedized EM mitigation (shielding, filtering, surge protection, etc.)…
  - which is sure to maintain very high levels of EM mitigation, despite anything/everything that might happen *over it's entire lifecycle*…
- I call this the 'Big Grey Box' (BGB) approach…
  - it works very well, but can be too large, heavy or costly for many modern safety-related systems…
  - e.g. in avionics, automobiles, portable or implantable medical devices, etc.

14 of 47


Some BGB examples


CCC
Overview of the IET's new guidance on T&Ms for EMC for Functional Safety
Comply with the usual, relevant EMC standards for functionality, over the complete lifecycle
Apply IEC 61508 design Techniques & Measures (T&Ms) appropriate for EMI (improved where necessary) to reduce residual risks
Overall result: EMI Resilience
Functional Safety should not be compromised by EMI, over the complete lifecycle
Use good EMC engineering at all levels of design
16 of 47

CCC

I think of EMI Resilience like this:

- **Passing the normal immunity tests means most EM disturbances don't cause EMI…**
  - **but extreme, unusual, unforeseen, simultaneous, etc. EM disturbances (i.e. beyond what is covered by the test standards) *or degradations in shielding, filtering, suppression, etc.,* cause EMI to occur**
- ***EMI means:* actual errors, malfunctions, faults in signals, data, control and/or power supplies…**
  - **which are detected by using appropriate T&Ms…**
  - **then either corrected (so operation continues safely-enough, perhaps with some functional degradation)…**
  - **or else the EUC is switched into a "safe state"**

17 of 47

CCC

61508 T&Ms for "EMI Resilience"

- **61508 lists many design T&Ms for detecting and/or correcting errors, malfunctions, faults, etc. in hardware (61508-2) and software (61508-3)…**
  - **to reduce their risks to the degree required to achieve the target functional safety risk…**
    - **and functional safety designers / assessors are very experienced with them**
- **The IET's new guidance lists which of these T&Ms are good for dealing with EMI effects…**
  - **and how to make them work better for EMI…**
  - **which will not require functional safety designers or their independent assessors to learn much more**

18 of 47

CCC

Examples of EMI Resilience T&Ms: System Design

- Physically separating safety functions from non-safety functions
- Specification of system requirements and design approaches, including (for example):
  - redundancy and diversity
  - error detection and error correction
  - static and dynamic self testing
- Integration of subsystems, power supplies and communication links
- Fault monitoring and recording (to help identify causes of malfunctions and improve future designs)

19 of 47

CCC

Examples of EMI Resilience T&Ms: Redundancy and Diversity

- multiple sensors sense the same parameters
- multiple copies of data are stored…
- multiple communications carry the same data…
- multiple processors process the same data…
- with comparison (error detection) or voting e.g. any two that agree out of three (error correction)

- All these can benefit from a wide range of diverse technologies/techniques to improve their effectiveness against the common-cause failures typically caused by EMI

20 of 47

CCC

Examples of EMI Resilience T&Ms: Error Detection & Correction Codes

- Error Detection Coding (EDC)…
  - means detecting corrupt data by adding sufficient redundant data bits…
  - designed to make a sufficient number of simultaneous bit errors detectable
- Error Correction Coding (ECC)…
  - means adding enough redundant data to EDC, designed to restore data to the degree required
- The modern world (GSM, Internet, CDs, DVDs, TV, etc.) relies totally on EDC and ECC

21 of 47

CCC

Examples of EMI Resilience T&Ms: Static and Dynamic Self-Testing

- Static testing checks hardware and software *before* starting operation…
  - preventing start-up if necessary…
    - as long as this is a safe state, of course
- Dynamic testing checks that operation remains correct *during* operation…
  - critical aspects of data processing could even be checked for correctness every second…
    - perhaps even more often

22 of 47

CCC

Choosing EMI Resilience T&Ms

- Some "EMI Resilience T&Ms" will probably have already been chosen for other functional safety reasons…
  - and some of them may be able to be modified to improve EMI resilience…
  - but extra EMI Resilience T&Ms may have to be used to achieve sufficient EMI resilience overall
- In a system…
  - some items of equipment may rely on the IET's new EMI Resilience approach…
  - whilst others use the traditional BGB approach

23 of 47

CCC

EMC engineers have difficulty understanding Functional Safety

- Traditionally, EMC is proved by (costly) testing…
  - and we have seen that testing cannot possibly be sufficient to demonstrate a design will achieve safety risks in the low parts per million per year
- And immunity tests focus on whether EMI causes functionality to degrade by too much…
  - but Functional Safety engineering cares nothing for functionality! (however, see "availability" later)…
  - *even if EMI causes permanent damage…*
  - as long as safety risks remain low enough!

24 of 47

CCC

The need for EMC testing

- It is possible to rely solely on 61508 design T&Ms to create functionally safe systems…
  - but if they switch to their safe state too often they can suffer too much downtime, i.e. have unacceptably low availability
- Such systems should be expected to be modified by users/owners to reduce their downtime…
  - any subsequent dangerous failures would be *the manufacturer's fault…*
  - because such misuse is reasonably foreseeable

25 of 47

CCC

Adequate availability simply needs compliance with the normal EMC immunity standards…

- for the application and its EM environment(s)…
- i.e. the test standards already widely used for compliance with (for e.g.) the EMC Directive, or customer-specific EMC specifications (underground railways, automobile, military, etc.)…

- Our EMC community has *(of course)* great experience with doing this…
  - the IET's new guide requires them to learn how to design so that ***EMC standards compliance is maintained throughout the whole lifecycle***

26 of 47

CCC

Design verification and validation

- No single verification or validation method alone can provide sufficient *design confidence*
- So, to achieve the confidence required for the level of acceptable risk…
  - several different methods are applied to a system, hardware or software design…
    - by designers, to verify their designs…
    - by independent assessors, to validate a design

27 of 47

CCC

No one verification/validation method can provide sufficient confidence continued…

- IEC 61508 and its "daughter" standards provide detailed guidance on the methods considered appropriate…
  - for verifying/validating system, hardware and software design…
  - and functional safety designers and assessors have become very skilled in applying them
- But they generally need to be modified and/or extended to correctly deal with issues of EMI resilience

28 of 47

CCC

It is important for designers and assessors to understand that EMI can cause any signals, data and/or controls to suffer from…

- an almost infinite variety of degraded, distorted, delayed, re-prioritised, intermittent and/or false values…
- and similar *or different* degraded, distorted, *etc…* values occurring on one or more (possibly all) other signals, data and/or controls

29 of 47

CCC

It is *also* important for designers and assessors to understand that EMI can cause any AC or DC power supplies to suffer from…

- an almost infinite variety of waveform distortions, overvoltages, undervoltages (dips, dropouts, interruptions, etc.)
- *and* similar *or different* problems to occur on one or more (possibly all) power supplies

30 of 47

CCC

And it is *also* important for designers and assessors to understand that these EMI effects can all happen *simultaneously*…

- i.e. everything can go wrong at once…
  - possibly in different ways…
- or they can happen in *any* time sequence that could have a critical safety consequence

31 of 47

CCC

Verification and validation approaches include…

A) Demonstrations

B) Checklists

C) Inspections

D) Walk-throughs

E) Reviews and assessments

F) Audits

G) Other approaches not listed here

32 of 47

CCC

Each of the approaches A) – G) can use some/all of the following techniques…

i) Inductive design analysis

ii) Deductive design analysis

iii) "Brainstorming" design analysis

iv) Test methods

v) Validated computer modelling

Plus – *specifically for EMC…*

vi) Non-standardised EM checks & tests

vii) Standardised EMC testing
(which can be extended to increase EMC design confidence)

33 of 47

CCC

Dealing with EMI in inductive, deductive and brainstorming analyses

- None of the standard methods were developed for EMI…
  - so to achieve 'due diligence' in covering all of the reasonably foreseeable possibilities for EMI to give rise to safety hazards…
  - it is necessary for people with appropriate competencies to adapt the chosen methods…
  - including during brainstorming

34 of 47

CCC

Extending the standard EMC tests to improve design confidence

- **Repeat the standard (or extended, see later) EMC tests on units after they have undergone various kinds of accelerated ageing…**
  - **usually *highly* accelerated to simulate the effects of different environments over the entire lifecycle…**
  - **to help ensure that the EM mitigation (shielding, filtering, suppression, etc.) will not degrade by too much over the entire lifecycle**

35 of 47

CCC

Extending the standard EMC tests to improve design confidence continued…

- **Standard EMC immunity tests can usefully be extended by using:**
  - **increased frequency ranges (lower and higher)…**
  - **higher test levels…**
  - **more angles/polarisations in radiated testing…**
    - **e.g. using mode-stirred / reverberation chambers…**
  - **frequencies that a design is especially susceptible to…**
    - **stimulated either by the CW frequencies themselves, and/or by demodulation, and/or by intermodulation**

36 of 47

CCC

Laboratory testing continued…

- During any testing, *all* variations in functional performance should be recorded…
  - and analyzed afterwards…
  - to see if they could have any possible relevance for safety risks for the overall safety-related system
- This is an especially powerful technique when building a system from individual units…
  - where only the individual units can be fully EMC tested in a laboratory…
    - note that *in-situ* (*on-site*) EMC immunity testing of the complete system, to some extent, is often practical

37 of 47

CCC

Let's be perfectly clear about this!

- The ***only*** techniques that can prove that EM disturbances will not cause unacceptable functional safety risks, are either…

1. The traditional, well-proven BGB approach…
   - i.e. over-specified, rugged EM mitigation, *or*…
2. The IET's 2013 guide on achieving EMI Resilience by using 61508's T&Ms…

   www.theiet.org/factfiles/emc/emc-overview.cfm...
   - chosen and/or modified as required…
     - or other design/verification/validation T&Ms with equivalent effects

38 of 47

CCC

Managing functional safety (and other) risks caused by EMI needs much more than immunity testing

An introduction to the IET's 2013 guidance on "EMI Resilience"

the end

Keith Armstrong, C.Eng., FIET, Senior MIEEE, ACGI

CHERRY CLOUGH CONSULTANTS LTD

www.cherryclough.com

39 of 47

CCC

Some references

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

40 of 47

CCC

Some references continued…

- **"We no longer have the luxury of carefully testing systems and designs to understand all the potential behaviours and risks before commercial or scientific use."**
  - **an extract from: "A New Accident Model for Engineering Safer Systems," by Professor Nancy Leveson, Professor of Aeronautics and Astronautics, and Professor of Engineering Systems, Massachusetts Institute of Technology (MIT), USA, in: "Safety Science," Vol. 42, No. 4, April 2004, pp. 237-270: http://sunnyday.mit.edu/accidents/safetyscience-single.pdf**

41 of 47

CCC

Some references continued…

- **"With autonomous driving new questions arise. To do automated braking you need a certain amount of validation. We have looked at what it takes to validate autonomous driving, and the time needed was estimated at 100,000 years. We need breakthrough solutions from the research community."**
  - **a quote from Michael Bolle, president of Corporate R&D at Robert Bosch, from "Car safety and the digital dashboard" by Chris Edwards, in E&T, the magazine of Institution of Engineering & Technology, vol. 9, iss. 10, 13 October 2014, http://eandt.theiet.org/magazine/2014/10/car-safety.cfm**

42 of 47

CCC

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

43 of 47

CCC

Some references continued…

- **"If you go to the Museum of Science and Industry in Manchester… …You stand there looking at the rods and the cogs and the flywheels pumping and churning away and you think, "*That piston will hit that wheel next time round*." But it never does. Everything misses everything else by exactly the same margin every time. For ever.**
  Electrical equipment, however, is different. It can do the same thing over and over and over again, but then one day it will just freeze and you have to turn it off and then on again, or tap the viewing card with your teeth, or unplug the system and leave it be for three minutes."
  - **an extract from: "A brilliant feat of pointless engineering? Guilty as charged," by Jeremy Clarkson, presenter of the Top Gear TV show, in 'Driving', Sunday Times, 12 January 2014, page 10, www.thesundaytimes.co.uk/sto/ingear/clarkson/article1360561.ece**

44 of 47

CCC

Some references continued…

- **For many very useful free HSE publications on Risk Assessment, visit www.hse.gov.uk/pubns and search by "ALARP risk assessment"**
  - **the most relevant documents will appear on the first and second pages of results, and can be downloaded as PDFs**
- **IEC 61508 "Functional Safety of Electrical/Electronic/ Programmable Electronic Safety-Related Systems" in seven parts, from https://webstore.iec.ch and other providers**
- **"Why few (if any) medical devices comply with their EMC standard, and what can be done about it" by Keith Armstrong, IEEE 2014 International Symposium on EMC, Raleigh, NC, Aug3-8, ISBN: 978-1-4799-5543-5**

45 of 47

CCC

Some references continued…

- **"Why increasing immunity test levels is not sufficient for high-reliability and critical equipment" by Keith Armstrong, IEEE 2009 International Symposium on EMC, Austin, TX, August 17-21, ISBN: 978-1-4244-4285-0**
- **"Why EMC Immunity Testing is Inadequate for Functional Safety" by Keith Armstrong, IEEE 2004 International Symposium on EMC, Santa Clara, CA, August 9-13, ISBN: 0-7803-8444-X**
- **"Overview of techniques and measures related to EMC for Functional Safety" published by the IET in Aug 2013, free download from: www.theiet.org/factfiles/emc/emc-overview.cfm**
- **"Testing for immunity to simultaneous disturbances and similar issues for risk managing EMC" by Keith Armstrong, IEEE 2012 International Symposium on EMC, Pittsburgh, PA, August 5-10, ISBN: 978-1-4673-2059-7**

46 of 47

CCC

Some references continued…

- **"Developing Immunity Testing to Cover Intermodulation" by Dipl. Ing. (FH) Werner Grommes and Keith Armstrong, IEEE 2011 International Symposium on EMC, Long Beach, CA, August 15-19, ISBN: 978-1-45770810-7**
- **"Details of the first practical method for Risk-Managing EMC" a half-day workshop by Jeffrey Silberberg and Keith Armstrong, IEEE 2014 International Symposium on EMC, Raleigh, NC, Aug 3-8, ISBN: 978-1-4799-5543-5**
- **"EMC Risk Management"**
  a half-day workshop by Jeffrey Silberberg and Keith Armstrong, IEEE 2015 Symposium on EMC&SI, Santa Clara, CA, March 15-21, ISBN: 978-1-4799-1991-8

47 of 47