FSemc15 v1.1

CCC

Resilience to Electromagnetic Disturbances

for reducing functional safety and other risks

Eur Ing Keith Armstrong CEng, FIET, Senior MIEEE, ACGI
phone & fax: +44 (0)1785 660 247
keith.armstrong@cherryclough.com
www.cherryclough.com www.emcstandards.co.uk

1 of 28

FSemc15 v1.1

CCC

EMI can be a cause of Functional Safety risks in electronic systems (in hardware and/or software)

- But this is not addressed in any detail by the basic standard on Functional Safety, IEC 61508…
  - nor by the product standards developed from it…
  - nor by ISO 14971 for the risk management of medical devices, equipment and systems
- So IEC 61000-1-2:2016 has been created to cover these omissions…
  - and the IET's new Code of Practice provides practical, detailed guidance on complying with it

2 of 28

FSemc15 v1.1

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 (including 'firmware')

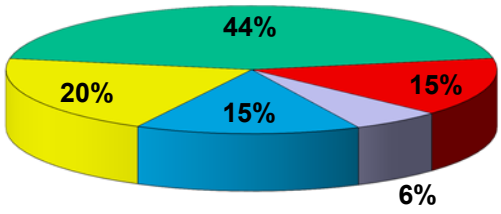
3 of 28

FSemc15 v1.1

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%

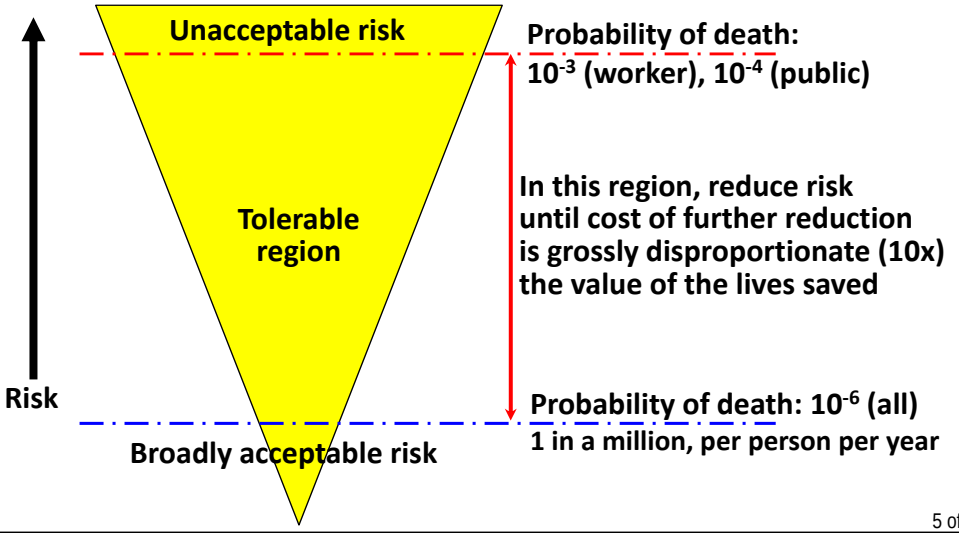
} > 60% of all failures are *built-in*

4 of 28

FSemc15 v1.1

CCC

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



5 of 28

FSemc15 v1.1

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 (even Microsoft can only *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

6 of 28

FSemc15 v1.1

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"

7 of 28

FSemc15 v1.1

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

8 of 28

FSemc15 v1.1

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

9 of 28

FSemc15 v1.1

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)

10 of 28

FSemc15 v1.1

CCC

The first practical method for risk-managing EM disturbances…

- Published by the IET in 2013: "Overview of Techniques and Measures Related to EMC for Functional Safety",
  - download: www.theiet.org/factfiles/emc/emc-overview.cfm
  - included in IEC 61000-1-2:2016 as Annex B…
  - planned to be added to Annex F of IEC 60601-1-2 Edition 4:2014 at its Amendment 1, in 2019…
  - in development as draft IEEE P1848: "Techniques and Measures for the Risk Management of Electromagnetic Disturbances"

11 of 28

CCC

IET Standards

Code of Practice
for Electromagnetic
Resilience

Jan 2017: published as the IET Code of Practice on "Electromagnetic Resilience"

12 of 28

FSemc15 v1.1

CCC

The traditional way of achieving EM Functional Safety despite an unknown EM environment…

- …is to use over-specified and ruggedized EM mitigation (shielding, filtering, surge protection, etc.)…
  - which is competently maintained, hence certain to provide high levels of EM mitigation over it's lifecycle
- This approach works well, but can be too large, heavy, costly for modern safety-related systems…
  - e.g. domestic appliances, avionics, power tools, automobiles, medical devices, etc…
  - and the IET's new CoP is the first (and only) practical alternative at this time

13 of 28

FSemc15 v1.1

CCC

Examples of products using high-spec., ruggedized EM mitigation

14 of 28

FSemc15 v1.1

Overview of IET's new CoP

CCC

Good EMC and functional safety engineering practices used throughout the design, including appropriate techniques and measures

Compliance with EMC test standards for emissions and immunity applicable to the normal EM environments expected to be experienced – *over the lifecycle (assuming no faults)*

Appropriate additional practices, techniques & measures are used to ensure risks remain tolerable – *despite reasonably foreseeable EM disturbances and faults over the lifecycle*

Result:
EM Resilience

The safety integrity achieved is sufficiently resilient to all reasonably foreseeable EM disturbances and faults over the lifecycle

15 of 28

FSemc15 v1.1

'EM Resilience' works like this:

CCC

- **Passing all relevant immunity tests *throughout the entire lifecycle* means that *most of the usual* EM disturbances won't cause EMI…**
  - **but extreme/unusual/simultaneous EM disturbances or degradations/faults (including failures in EM mitigation), could still cause EMI**
- ***EMI means* actual errors, malfunctions, or faults in signals, data, control, or power supplies…**
  - **which are detected by the appropriate T&Ms…**
  - **then either corrected (so that operation of the equipment continues with low-enough risks)…**
  - **or else the equipment is switched into a safe state**

16 of 28

FSemc15 v1.1

CCC

T&Ms for 'EM Resilience'

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

17 of 28

FSemc15 v1.1

CCC

The IET's new CoP lists T&Ms for improving EM Resilience in…

- System and Operational design
- Managing the EMC design to prevent errors, malfunctions and faults from occurring
- Error detection and/or correction during operation, by redundant channels, data coding, self-testing, etc.
- Verification and validation of the design
- Fault monitoring and recording, for diagnosis and improvement
- Maintenance, repair, refurbishment, upgrade, etc.
- Etc…

18 of 28

FSemc15 v1.1

CCC

Overviews of some examples of EM Resilience T&Ms

- 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
- 'EM-aware' integration of subsystems, power supplies and communication links
- Fault monitoring and recording (to help identify causes of malfunctions and improve future designs)

19 of 28

FSemc15 v1.1

CCC

Redundancy and diversity T&Ms?

- Use of redundant paths ('channels') is a technique that has long been used in High-Reliability and Functional Safety engineering…
  - however, redundancy is traditionally achieved using a number of identical channels
- Such redundant systems can cope with random failures (e.g. failed components)…
  - but EMI is a *systematic common-cause failure mode*:
    - *systematic:* a given system design will always behave in the same way when a given EM disturbance is applied…
    - *common-cause:* EM disturbances influence identical components/designs in the same way

20 of 28

FSemc15 v1.1

CCC

So we need to use technological diversity in any redundant 'channels'...

- 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)…
- using a wide range of different (diverse) technologies and techniques in the design of hardware and software, *and* in their verification and validation…
- to improve their effectiveness against the common-cause failures caused by EM disturbances

21 of 28

FSemc15 v1.1

CCC

Overview of some error correction/detection T&Ms

- Error Detection Coding (EDC)…
  - adding sufficient redundant bits to the data, to make it possible to detect a sufficient number of simultaneous bit errors in the original data
- Error Correction Coding (ECC)…
  - adding a sufficient number of redundant bits to make it possible to restore erroneous data, to the degree required
- The modern world (cellphones, Internet, CDs, DVDs, flash memories, SSDs, digital radio and TV broadcasting, etc.) relies totally on EDC and ECC

22 of 28

FSemc15 v1.1

CCC

Overview of some static and dynamic self-testing T&Ms

- Before starting-up a process, the contents of the program and data memories are checked for correctness (e.g. using EDC such as checksums)…
  - if a memory doesn't pass, ECC recovers correct data, or a diverse memory that *does* pass its static tests is used (redundancy)
- Whilst running a process, known signals/data are continually interleaved with *real* signals/data…
  - and outputs checked against what *should* result…
    - if a test isn't passed, either ECC recovers correct signals/data or a diverse process is used that *does* pass these dynamic self-tests (redundancy)

23 of 28

FSemc15 v1.1

CCC

Some more T&Ms

- Verification and validation require a range of techniques, *including* EMC testing (which cannot be sufficient on its own for human safety or other critical risks)…
  - but EMC testing *can* be developed to be much more valuable in demonstrating that a design has adequately low risks…
  - with the potential for a lot of interesting work in developing customised tests and bespoke test plans for risk-reducing individual systems / applications
- This has been a very brief overview…
  - there are also recommended T&Ms for power supplies

24 of 28

FSemc15 v1.1

CCC

Choosing sufficient T&Ms for a sufficient level of EM Resilience

- Some good EM Resilience T&Ms will probably have been chosen for other risk-reduction reasons…
  - and might be modified to improve EM Resilience
- Additional EM Resilience T&Ms may need to be applied to achieve sufficient EM Resilience…
  - for the level of safety (or other) risk being aimed for
- In a system, some items of equipment may use the T&Ms for EM Resilience approach…
  - whilst others use traditional over-specified, ruggedized, competently maintained EM mitigation

25 of 28

FSemc15 v1.1

CCC

Summary and Conclusions

- EMC for Functional Safety *cannot* be achieved by immunity testing alone…
  - however much the test levels are increased!
- EMC for Functional Safety *cannot* be achieved solely by improving EMC skills or expertise…
    - unless relying on the traditional "over-spec'd mitigation" method…
  - however, improvements in EMC skills/expertise ***are*** generally needed…
  - to ensure the usual EMC tests would be complied with over the entire lifecycle…
    - to help ensure availability, reduce downtime

26 of 28

FSemc15 v1.1

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 approach** (over-specified, ruggedized, competently-maintained EM mitigation) ***or…***
2. **The IET's new CoP on achieving EM 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

27 of 28

FSemc15 v1.1

CCC

Resilience to Electromagnetic Disturbances

for reducing functional safety and other risks

the end

Eur Ing Keith Armstrong CEng, FIET, Senior MIEEE, ACGI
phone & fax: +44 (0)1785 660 247
keith.armstrong@cherryclough.com
www.cherryclough.com www.emcstandards.co.uk

28 of 28