The Dark Art and Safety Related Systems

EMC for Functional Safety
IRSE Seminar 28th January 2014

Presentation by Ken Webb
Commonly held views about EMC,

- “It’s an Arcane discipline”
- “It’s all Black Magic”
- “Don’t invite EMC Engineers to Dinner Parties”

The enlightened view of EMC,

- Current Management
  - Minimise Coupling
- Frequency Management
  - Design for EMC
The IET 2013 Guide in context

IEC 61508, *Functional Safety of Electrical/Electronic/Programmable Electronic (E/E/PE) Safety Related Systems*

IET Guide on Overview of techniques & measures related to EMC for Functional Safety, 2013

DD IEC/TS 61000-1-2:2008, *Methodology for the achievement of functional Safety of Electrical and Electronic Systems including equipment with regard to electromagnetic phenomena*

What is Functional Safety?

**Functional safety**: part of the overall safety that depends on a system or equipment operating correctly in response to its inputs.

[IEC 61508-4, modified]

**Examples:**
- Safety achieved by reliance on *passive* systems
  e.g. fire resistant doors is *not* functional safety
- Safety achieved by reliance on *active* systems
  e.g. detection of trains and intelligent activation of signals
  *is* an example of functional safety
EMC for Functional Safety -
Failures caused by EMI are “Systematic”

- Depends upon the design (i.e. a given design in a given state will behave the same way when a given EMI threat is applied) - they are not random.
- We can’t use the traditional risk-reduction techniques that have been developed for reliability engineering instead, for compliance with EN 61508 (and EN50126/28/29), we must achieve appropriate **EMC design confidence.**
Key Points covered in the Presentation

- The Railway Electromagnetic Environment
- EMC for Functional Safety – the challenges
- The IET Guide - Overview of techniques and measure related to EMC for Functional Safety
The Railway Electromagnetic Environment
Rolling Stock example of EMC Interfaces – Internal and External

- Radiated EMI
- Incident EMI
- Conducted EMI
- Compatibility between trains and track circuits
- Induction
- Compatibility with axle counters and line side telecommunications

INTRA EMC

Apparatus A

Apparatus B

Traction package
The changing railway Electromagnetic Environment

- Harmonics - Variable frequency inverter drives
- In – cab Signalling, ERTMS
- Selective Door Opening (SDO)
- Public demand for on board WiFi
- The proliferation of mobile phones and portable electronic devices (PED) e.g. laptop computers, tablets/iPads, MP3 players/iPods, e-readers/Kindles and all types of gaming devices used by the travelling public within the railway environment.
EMC for Functional Safety – the challenges
EMC Safety Case consists of 3 key deliverables

   - BS EN 50121 series

2. Engineering Acceptance
   - Railway Group Standards GE/RT8015 and GE/RT8270

3. EMC Safety Submission
   - BS EN 50122 series
   - BS EN 50238
   - IDI 500xx series

EMC Strategy for Network Rail – NR/L1/RSE/30040
EMC Assurance Process for Network Rail - NR/L2/RSE/30041
EN 50121-4 does not prescriptively cover all Railway EM phenomena

- Track circuits
- Traction current harmonics
- Microwave Communications
- Radar

Frequency range of EN 50121-4:

- 0Hz
- 150kHz
- 2.5GHz

Frequency
The Electromagnetic Environment over the lifecycle of the Safety Related Product

All EM Phenomena

EM phenomena \textit{not} covered by EN 50121-4
- Fault conditions
- Safety Related
- Traction current induced

EM phenomena covered by EN 50121-4
“Special situations” where disturbance greater than, or additional to, levels in EN 50121-4

<table>
<thead>
<tr>
<th>More EMC Testing?</th>
<th>Mitigation techniques?</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Increase levels 30V/m?, 40V/m?</td>
<td>▪ Filtering?</td>
</tr>
<tr>
<td>▪ Multiple threats? CW and transients?</td>
<td>▪ Surge suppression?</td>
</tr>
<tr>
<td>▪ Effects of physical environment and ageing?</td>
<td>▪ Shielding?</td>
</tr>
<tr>
<td>= Time and ££££££££!!!!</td>
<td>= Weight, footprint, components and ££££££££!!!!</td>
</tr>
</tbody>
</table>
SIG - Industry adoption of Commercial Off The Shelf (COTS) Electronic Control Systems

- Lower cost than bespoke
- Tried and tested technology

Lower EMC performance
- e.g. V/m, A/m, surge/transient
- than Rail industry requirements
EMC for Functional Safety
Summary of the main challenges

- Placing reliance solely on EMC testing to EN 50121-4 will not guarantee functional safety of safety related equipment.

- Determining the “reasonably foreseeable worst-case EM environment” over the lifecycle of the equipment (30 years?) is a very big challenge.

- Traditional EMC mitigation techniques e.g. shielding can be costly and impractical.

- EMC performance of COTS equipment used in signalling projects may be lower than EN 50121-4.
The IET Guide
Overview of techniques and measure related to EMC for Functional Safety
Techniques and Measures related to EMC for Functional Safety – the IET Working Group

- IET WG on EMC for Functional Safety
- Published 3 Professional Guidance Documents
- WG formed of Industry Experts:
  - Rail
  - Process
  - Defence
  - HSE
The Aim of the IET Guide

- To provide a non-exhaustive range of techniques and measures to address the effects of EMI that a safety related system could experience over its lifecycle.
- Part of the evidence required for functional safety arguments and for compliance with EN 61508 (and EN 50126/28/29).

The Guide supplements the information provided on EMI in the following standards and guidance,

- IEC 61508 (EN 50126/28/29)
- IEC 61000-6-7
- IET’S 2008 Guide on EMC for Functional Safety
The Purpose of the IET Guide

The Guide has been developed specifically to help overcome the following difficulties:

- Impracticality of performing a complete assessment of the EM environment over the lifecycle of the safety related system
- Use of heavy and costly EMC mitigation techniques e.g. shielding, filtering etc
Approach taken by the IET Guide

1. Apply good EMC Engineering Practice during Design
2. Apply additional EMC Techniques and Measures in Design, Verification and Validation as necessary
3. Compliance with applicable EMC Standards as a basis e.g. EN 50121-4
4. Evidence for Safety Case Can be accepted as adequately safe for EMC
IET Guide - Guidance based on classification

- **Detection** – effectiveness to reveal the presence of an error or malfunction that could be due to EMI.

- **Mitigation** – behaviour of the safety function in response to the detected errors or malfunction that could have been caused by EMI.

- **Importance (for SILs)** – incorporates the necessity and/or desirability of the Detection and/or Mitigation technique or measure with the following attributes:

<table>
<thead>
<tr>
<th>None</th>
<th>Not Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Recommended</strong></td>
<td><strong>Highly Recommended</strong></td>
</tr>
</tbody>
</table>
IET Guide - Range of Techniques and Measures

- Project Management
- Specification
- System Design
- Operational Design
- Implementation
- Verification and Validation
<table>
<thead>
<tr>
<th>Section number in IET Guide</th>
<th>Equivalent in Annex A</th>
<th>Equivalent in Annex B</th>
<th>Equivalent in Annex C</th>
<th>No Equivalent in</th>
</tr>
</thead>
<tbody>
<tr>
<td>IET Guide</td>
<td>IEC 61508-7</td>
<td></td>
<td></td>
<td>8 additional EMC techniques and measures</td>
</tr>
</tbody>
</table>
Detecting excessive RF on AC or DC power supplies

**Aim:** To detect the presence of excessive RF on power supplies.

**Detection:** Triggering of dedicated RF detector

**Mitigation:** If, during time $t$, EMI does not disappear, apply appropriate response

**Importance:** R for SIL 1 and 2, HR for SIL 3 and 4
IET Guide - Conclusions

- Adoption of good EMC engineering practice during design.
- Compliance with the normal immunity tests e.g. EN 50121-4 for functionality over the lifecycle
- Hardware and software T&Ms that ensure EMI does not cause unacceptable safety risks
  - can provide smaller, lighter and less-costly safety-related systems
  - no need to try to determine worst-case EM environments over the future lifecycle
Thank you for your attention

- Copies of the Guide are available today!
- Your feedback on the Guide is encouraged and will be welcomed.
- SIL ratings – importance for EMC. Discuss!!
- A comparison with EN 50129 Techniques & Measures?
- Contact details as follows:

  Email: Ken.webb@mottmac.com
  Mobile: 07791 871891
Additional slides not part of main presentation
Commercial EMC Test standards have a complex hierarchy

- **Basic standards**
  - Examples
    - EN 61000-3-XX
    - EN 61000-4-XX

- **Product specific**
  - Examples
    - EN 50121-4
    - EN 50293
    - EN 50270

- **Product family**
  - Examples
    - EN 55011
    - EN 55022
    - EN 55024

- **Generic**
  - EN 61000-6-XX
Railway Communication, Signalling and Processing Systems – Safety related

- EN 61508-1 replaced by EN 50126/EN 50128/EN 50129 for railways

- EN 50129
  - Annex B references EN 50121-4 to be *used as a basis for EMC*
  - Annex E Techniques & measures described for SIL levels includes EMC

- EN 50121-4 is the harmonised standard under EMC Directive 2004/108/EC
Achieving EMC for Functional Safety - Learning from the rail industry

• Certain railway infrastructure equipment has unique compatibility requirements beyond the scope of EN 50121 series of Railway EMC standards

• EE&CS (Electrical Engineering & Control Systems)

• Railway industry has used a risk based approach to signalling compatibility for many years

• Safety engineering in rail well defined - Yellow Book 4 Engineering Safety Management - ALARP principle
Aim of the Guide – to provide a range of T&M to address effects of EMI
What is a Safety Related System?

Designated system that,

- Implements the required safety functions necessary to achieve or maintain a safe state for the equipment under control, and

- Is intended to achieve, on its own or with other E/E/PE safety related systems, other technology safety related systems the necessary safety integrity for the required safety functions

[IEC 61508-4, modified]
Functional Safety Risks due to EMI

Where EMI causes errors, malfunctions or failures in the correct functioning of electronics (hardware or software), which can in turn increase functional safety risks.

The basic IEC publication covering this issue is IEC TS 61000-1-2:2008.

Note: this is not concerned with compliance with the EMC Directive or other EMC regulations; only with functional safety risks.

Risk Reduction

Requires Design Measures from Concept to Completion