The Safety-Critical Systems Club Newsletter

Safety Systems

Vol 27 No. 2 - October 2019

THE HUMAN FACTOR
Integrating human factors in safety management



RUNNING INTERFERENCE
Managing the risks of EMI

For everyone working in Systems Safety

SCSC

scsc.uk



SCSC Publication Number: SCSC-155

While the authors and the publishers have used reasonable endeavours to ensure that the information and guidance given in this work is correct, all parties must rely on their own skill and judgement when making use of this work and obtain professional or specialist advice before taking, or refraining from, any action on the basis of the content of this work. Neither the authors nor the publishers make any representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability or availability with respect to such information and guidance for any purpose, and they will not be liable for any loss or damage including without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever (including as a result of negligence) arising out of, or in connection with, the use of this work. The views and opinions expressed in this publication are those of the authors and do not necessarily reflect those of their employers, the SCSC or other organisations.

Except where explicitly stated that licensed use of this work is otherwise restricted, this work is licensed under the Creative Commons Attribution 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by/4.0/ or send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA. You are free to share the material in any form and adapt the material for any purpose providing you attribute the material to the Safety-Critical Systems Club (SCSC) newsletter, reference the source material, include the licence details above, and indicate if any changes were made. See the license for full details.

Contents

WELCOME

Editorial 3

Opening words from the new SCSC Newsletter Editor.

In Brief 5

Recent system safety news items from around the world.

FEATURES

Human Factors Integration: Technical Guide for Human Factors and Safety Management 7

David Pennie discusses recent guidance on the integration of Human Factors with Safety Management.

Why do we need new standards for EMI Functional Safety Risks? 17

Keith Armstrong and Davy Pissoort discuss the need for standardisation in Electromagnetic Interference (EMI).

Risks caused by Electromagnetic Interference 25

Keith and Davy go on to discuss the management of Functional Safety Risks arising from EMI.

Hardware and Software Techniques and Measures to Effectively Manage EMI Functional Safety Risks 33

Keith and Davy conclude their series of articles with details on specific techniques and measures to manage EMI safety risks.

GROUPS

Working Groups 44

Details of the current SCSC Working Groups.

SCSC Steering Group 47

Contact details for members of the SCSC Steering group.

EVENTS

Calendar 48

Events Diary 49

THE SAFETY-CRITICAL SYSTEMS CLUB, Seminar:

Data Safety Evolution

Thursday 14 November, 2019 - London, UK

The impact of data on safety systems is now well recognised and several high-profile accidents have had significant data causes or contributions. Data can directly cause systems to behave anomalously (for instance sensor data in the recent Boeing 737 MAX accidents) or it can cause humans to take inappropriate actions leading to harm (for example the loss of the Sikorsky S-92A helicopter in Black Rock, Co. Mayo, Ireland).

This seminar will look at what has changed in Data Safety in the last few years and where it is heading. It will consider the current status of guidance and standards in the area and also new developments. It will include talks from a variety of sectors where data safety is an important issue, in particular Healthcare, where data held in systems is crucial to effective diagnosis and treatment.

There will be a focus on the SCSC Data Safety Guidance document (https://scsc.uk/scsc-127D) and the software tooling being developed from it, enabling projects to easily work to the guidance.

There will be a panel session where the audience has an opportunity to put further questions to the speakers.

This seminar is an opportunity to hear about the issues data can cause in safety systems and look at new developments in the area. It will be useful for safety engineers and safety managers, across any sector that uses data in a safety context.

Talks include:

Mike Parsons, SCSC - "Why is data a safety problem?"

Mark Templeton, Qinetiq - TBC

Dale Calicott, BAE Systems - TBC

Divya Atkins, MCA - "Introduction to the SCSC Data Safety Guidance"

Paul Hampton, CGI - "Applying the SCSC Data Safety Guidance: Practical Considerations"

Martin Atkins, MCA - "Data Safety Tooling"

Alastair Faulkner, Abbeymeade - "Exploring the Data Safety Model (DSM) as part of the Assurance Solution"

The event is taking place at the Park Plaza Westminster Bridge London Hotel, Westminster Bridge Road, Lambeth, London, SE1 7UT, United Kingdom.

SCSC
FOR EVERYONE WORKING IN SYSTEM SAFETY

This seminar is an opportunity to hear about the issues data can cause in safety systems and look at new developments in the area.

It will be useful for safety engineers and safety managers, across any sector that uses data in a safety context.

Details at: www.scsc.uk

What is data safety about and where is it heading?

scsc.uk/e651

WWW.SCSC.UK

Editorial

Welcome to the new-look October 2019 edition of the Safety-Critical Systems Club Newsletter!

As announced recently on the SCSC website, I have now been appointed as the new Safety-Critical Systems Club's Newsletter editor, taking over from the great work that Katrina Attwood has been doing previously.

My thanks go out to Katrina for all her previous work and for gathering all the material to make this edition possible. I'm sure I speak for all the club members in thanking you for your hard work and wish you all the best for your future endeavours.

As I've been actively involved in publishing other SCSC documents, I thought I would take the opportunity to give the newsletter a more contemporary feel and my thanks go to Alex King for helping with the design.

The tie-in with the club's website will continue with plans to make mobile friendly versions of the newsletter available on the website.

There are some new additions to the newsletter: an 'In Brief' section on current news items relating to systems safety, details of the current SCSC Working Groups, details of how to connect to the club via social media and a contact section introducing readers to members of the SCSC Steering Group.

I would of course appreciate your feedback on the new format, which you can do by emailing me directly (address below) or you may like to include your thoughts on it in the new club survey that Mike Parsons has published. You can find the survey here:

scsc.uk/survey

I would encourage you to take a few moments to help shape the future direction of the Club by capturing your thoughts on the Newsletter and any other aspect of the Club. The survey is open to members and non-members alike and there is a chance to win some great prizes by completing the survey, including a free day at SSS'20.

This month's newsletter starts with David Pennie discussing recent guidance on the integration of Human Factors in Safety Management.

The remaining series of articles focus on the management of system safety risks arising from Electromagnetic Interference. Keith Armstrong and Davy Pissoort have provided three articles on this fascinating subject.

Paul Hampton
SCSC Newsletter Editor
paul.hampton@scsc.uk



SCSC

FOR EVERYONE WORKING IN SYSTEM SAFETY

Bookings at:
www.scsc.uk/events

This seminar is an opportunity to hear about what makes a good safety culture and how to create and maintain it through specific activities.

It will be useful for safety practitioners, safety managers, and for those involved in the management and training of staff in safety-related industries.

Details at: www.scsc.uk

How to cultivate the right attitudes in safety-related work

www.scsc.uk

THE SAFETY-CRITICAL SYSTEMS CLUB

Seminar: Creating and Maintaining an Effective Safety Culture

5th December 2019,
DoubleTree by Hilton Hotel London - West End

This seminar will consider how to create and maintain a strong and effective safety culture which is appropriate and relevant to an organisation's needs.

Safety culture is embodied in the attitudes, actions and behaviours of staff and has to be "owned" by the organisation. It is recognised that different industries may require different approaches depending on the safety risks they face, the regulatory environment and the staff they employ.

Of particular importance is to how to ensure resilience: there will always be knock-backs (e.g. due to organisational change and incidents or accidents) and the organisation must be able to recover its safety culture quickly. Also important is how to ensure the culture doesn't degrade, i.e. how to manage the indifference, complacency and poor attitudes and behaviours that can build up over time.

This seminar features seven talks from experts covering different sectors that operate effective safety cultures.

There will be a panel session where the audience to allow further interaction between the delegates and speakers.

scsc.uk/e631



In Brief








The Boeing 737 Max saga isn't even close to being over



Boeing has still not done enough to make its new jets flight-worthy. American Airlines have extended flight cancellations for Boeing 737 trips through to 3rd December, further highlighting the seriousness of the problems. *cnn.com*

37 People injured after Air Canada flight hits severe turbulence



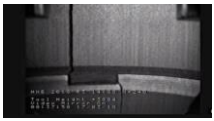
At least 37 people were injured on board an Air Canada flight to Sydney after the plane hit severe turbulence and had to make an emergency landing. *bbc.co.uk*



MOD drone crashed into tree after crew mix-up

A £6m military drone crashed after it landed beyond its planned touchdown point and hit a tree. The system computer failed to register it had landed so automatically powered up to attempt a go-around. However, the crew cut the power when the drone was 12m above the ground causing the crash. *bbc.co.uk*

Nuclear reactor to restart after 'cracks' closure



One of two nuclear reactors at the Hunterston B power plant, which were shut down last year, has been given permission to return to service.

Hundreds of cracks were found in the graphite bricks within the reactor cores at the North Ayrshire plant. The Office for Nuclear Regulation (ONR) has now agreed that it is safe for operator EDF to restart one of the reactors for a four-month period. *bbc.co.uk*

Russia's mysterious missile disaster suggest a "nuclear reactor blew up"



Russia's state weather agency has said that a cloud of inert radioactive gases, which swept across a Russian town in August, was produced by fast-decaying radioactive isotopes released by an explosion at the Nyonoksa testing range. Experts suspect it involved a failed test of Russia's new nuclear powered superweapon that NATO calls the SSC-X-9 Skyfall. *businessinsider.com*



US Army wants AI missiles that find their own targets.

AI may soon decide who lives or dies. The US Army wants to build cannon-fired missiles that will use AI to hunt their targets, out of reach of human oversight. *newscientist.com*

Seminar: Safe Use of Multi-Core and Manycore Processors

THE SAFETY-CRITICAL SYSTEMS CLUB, Seminar:

Safe Use of Multi-Core and Manycore Processors

Thursday 30 April, 2020 - London, UK

This seminar will consider how to use processors with multiple cores in a way that safety can be assured, and such that the resulting system can be certified against industry standards and guidelines.

(A **multi-core** processor is typically made of several independent processor cores on the same chip, connected through an on-chip bus. **Manycore** processors are specialist multi-core processors designed for a high degree of parallel processing, containing a large number of simpler, independent cores (from a few tens of cores to thousands or more). Manycore processors are used extensively in embedded and high-performance computing.)

This seminar will be held in central London.

Speakers include:

Iain Bate, University of York - "Multi-core architectures and timing analysis: Their influence on the scheduling of certifiable real-time systems"

TBC, Lynx Software Technologies - TBC

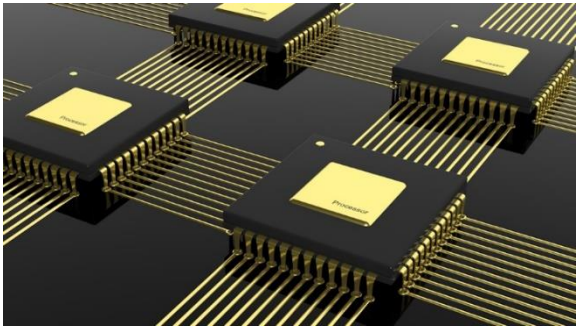
Guillem Bernat, Rapita Systems - "Independently Verifying the effectiveness of RTOS Hypervisors at reducing Multicore Interference"

TBC, Wind River - TBC

Mark Headley and Mike Standish, Dstl - "A strategy for Multi-Core Qualification"

Further details TBA.

scsc.uk/e638



Human Factors Integration: Technical Guide for Human Factors and Safety Management

	RACI Matrix			
PSI Objectives	**Responsible**	**Accountable**	**Consulted**	**Informed**
Appoint a person responsible for HF (the HFIF) within the DT.	*DTL*	*DTL*	*PSM*	*Other DT members*
Identify the key contacts and define roles and responsibilities.	*HFIF*	*DTL*	*PSM*	*Other DT members*
Understand HF within the programme through an initial scoping and proportionality review.	*HFIF*	*DTL*	*DTL, PSM, Other DT members*	*Other DT members*
Determine whether the HFIF is a Safety Management stakeholder and/or required on the PSC.	*PSM*	*DTL*	*HFIF*	*Other DT members*
Communicate the role of HF to the DT.	*HFIF*	*DTL*	*PSM*	*Other DT members*

David Pennie discusses recent technical guidance that has been published by the MOD on improving integration of Human Factor considerations in System Safety Management.

The Integration of Human Factors (HF) with Safety Management (SM) in high hazard sectors, such as nuclear, rail and oil and gas has been instigated by significant and high-profile accidents such as: Windscale (1957), Three Mile Island (1979), Chernobyl (1986), Flixborough (1974), Piper Alpha (1988) and Clapham (1988). These accidents led to significant changes in Safety Case (SC) legislation.

1988 Piper Alpha disaster (petrochemical). An oil platform that was later converted to gas production. An explosion on the platform and the resulting fire killed 167 men with only 59 survivors. The publication in 1990 of Lord Cullen's report into the Piper Alpha disaster paved the way for the introduction of formal safety case requirements in the UK offshore industry. In 1992 Safety Case Regulations (SCR) were adopted for UK offshore industry.

Over time and with greater knowledge and understanding of accident causation there has been an increasing requirement for the comprehensive integration of HF and SM within the SC regime. This is supported by institutions such as the Health and Safety Executive (HSE), who provide guidance, review SC documentation and carry out inspections.

Whilst notable accidents, such as Nimrod (2006), have occurred in the defence sector, it has not precipitated the same level of regulation. The reasons for this are multifaceted, complex and not entirely clear, but this has resulted in regulatory drivers from HF integration with SM in defence not being as strong as in other high hazard sectors. Despite this, MOD recognise the need to strive to enhance the integration of HF and SM from within and identified that the way to achieve this was through the development of new guidance. It also recognised that there was the opportunity of learning from and applying Relevant Good Practice from other sectors.

A new publication titled: "Technical Guide for Human Factors and System Safety", has therefore been developed and published on the Human Factors Integration Management System (HuFIMS) website on behalf of Defence and Equipment Support (DE&S) services to help better integrate HF with the MODs Project Oriented Safety Management System (POSMS). The POSMS has 13 Safety Management Procedures (SMPs) as follows:

- Project Safety Initiation (PSI)
- Project Safety Committee (PSC)
- Safety Planning
- Preliminary Hazard Identification and Analysis (PHIA)
- Hazard Identification and Analysis (HIA)
- Risk Estimation
- Risk and As Low As is Reasonably Practicable (ALARP) Evaluation
- Risk Reduction
- Risk Acceptance
- Safety Requirements and Contracts
- Hazard Log
- Safety Case (SC) and Safety Case Report (SCR)
- In-Service Safety Management System (SMS).

These TGs are available for free for those signed-up to the MOD Knowledge in Defence (KID) website. The development of HFI and SM TG demonstrates MOD commitment to positioning HF in a central role in safety management. It also recognises how developing the understanding and knowledge of System Safety assessors and Delivery Team Leads (DTL) on the human contributions to safety will be very beneficial.

The purpose of the TG

The purpose of the TG is to provide an across-services publication to help better integrate HF with the System Safety aspects of DE&S acquisition projects, by:

- Improving understanding about the benefits of effectively integrating HF and acquisition System Safety
- Providing specific advice on how to integrate HF with the POSMS
- Supporting alignment of the activities conducted by safety and HF specialists by increasing the awareness and understanding of each other's areas of responsibility
- Providing a summary of HF analytic tools and methods that support Human Factors Integration (HFI) with System Safety, along with links to more detailed information and guidance.

Study rationale - Overall Approach to develop guidance

This TG was produced by Greenstreet Berman Ltd (GSB) in collaboration with HuSys Ltd as part of the Defence Science and Technology Ltd Defence Human Capability Science and Technology Centre (DHCTSC) programme. The development of the TG was based on a multi-method approach to use several data gathering activities to develop an understanding of:

- How HF is currently integrated with SM in defence projects
- What guidance or information supports this integration
- What is done elsewhere - in other safety critical industries
- What information should be included in the TG
- How it should be presented.

Finally, the research to develop the TG also explored what else might need to happen to further integrate HF and SM.

Methodology

What does MOD currently provide – Initial Review

An initial review was carried out to explore the extent to which the MOD already provides guidance on the integration of HF with SM. The findings indicated that:

- The current suite of HuFIMS TGs provides 'general' good practice guidance that could be referenced as a source for use by HF experts when linking with SM, for example, to develop HF risk reduction
- Current TGs provide guidance on specific activities like Early Human Factors Analysis (EHFA) that could support 'Safety Planning' as well as helping to inform 'Preliminary Hazard Analysis (HAZAN)'
- The current suite of HuFIMS TGs does not, however, comprehensively cover the POSMS SMPs or the types of HF analytic tools to support safety assessment and SM decision-making.

Analysis Matrix

In addition to the initial review, more detailed analysis was carried out to identify HF in-puts/outputs/touchpoints relevant to each POSMS SMP to help inform where HF could most effectively support SM. This, in turn, indicated the information to be included in the TG.

The work to develop the Matrix was carried out in several phases, including a three-quarter day workshop to explore, discuss and agree the content of the Matrix with Subject Matter Experts (SMEs). The findings indicated that HF should be an integral part of all the POSMS SMPs with HF inputs in four key areas:

- Physical participation at formal meetings/sessions (e.g. attendance at Hazard Operability Study (HAZOP) sessions)
- Tangible formal input (i.e. outputs from HF analysis or assessment activity)
- Informal input (i.e. ad-hoc discussions between HFI and SM specialists)
- HFI activity being so closely aligned to the POSMS SMP process, such that it becomes fully integrated, leading to adaptation either of the whole process or a key element of the POSMS SMP.

Interviews

Interviews were conducted with HF and SM specialists (as well those covering roles such as Design, Engineering and Assurance) to explore how well current internal MOD processes (e.g. Policies, Procedures and Guidance) support HFI with SM for military systems acquisition.

Nine people, from six defence projects took part covering Land, Air and Maritime domains.

The findings from the interviews indicated:

- Most respondents wanted improved guidance on how HF integrates with SM
- Interviewees listed several areas where additional guidance would help support HF and SM, such as human error analysis
- Interviewees noted that there was limited regulation driving HFI with SM
- There seemed to be a lack of understanding of the application of human failure probabilities in Fault Tree Analysis and reliance on qualitative assessment
- Both HF and Safety SMEs consider there would be benefits from possessing a greater understanding of each other's roles.

Learning from other sectors

The aim of the review of other sectors was not to critique existing information or formally indicate and rate the value of guidance, but rather, to seek ideas and inputs to inform the development of the TG. In total, 42 guidance materials were identified. Of these, 25 were reviewed in more detail following the application of screening criteria.

The findings indicated that that the most value that the Defence sector could gain from advice provided from other sectors was in HAZID, HAZAN, risk estimation, risk reduction and ALARP Evaluation. Some limited additional advice was also provided concerning the development of Safety Cases (SCs) and the transition of safety assessment to In-Service SM.

"The findings indicated that that the most value that the Defence sector could gain from advice provided from other sectors was in HAZID, HAZAN, risk estimation, risk reduction and ALARP Evaluation"

Stakeholder engagement

The findings from the initial review, Analysis Matrix, interviews and learning from other sectors were collectively reviewed by the project team to support the development of the TG. Emergent ideas on the content and style of the TG were set out in a User Requirement Document and skeleton draft. These were reviewed during a 3-hour Face-to-Face workshop session. In total 10 people took part in the workshop representing HF and SM specialisms working for DE&S or embedded in defence projects.

The findings from the review and workshop indicated that there was broad agreement from the target audience, with the proposed structure, scope and form of the HF and System Safety TG. There was also agreement that the TG should be aligned to the 13 POSMS SMPs. Other more specific comments were incorporated into the development of the TG.

Staged approach to TG development

The TG was delivered to stakeholders at the following stages in its development:

- Skeleton draft
- 20% complete
- 90% complete
- 100% complete – completed and proof-read document.

Following delivery of each draft, stakeholders were given the opportunity to comment on the TG. This staged approach helped to ensure that stakeholder had early sight of the document, ensuring its development was in line with their expectations and requirements. This was considered particularly important given the dual nature of the intended audience.

What the TG contains

Intended audience

The TG is primarily aimed at both HF and SM specialists working within the DE&S acquisition community, who support the design, specification, assurance, purchase and supply of Product (e.g. weapons, platforms): System and Services (PSS).

It is also aimed at other Project-based team members who interface with HF and SM or, who have a vested interest in effective SM (e.g. the Delivery Team Leader (DTL), Principal/Chief Engineer, Requirements Managers etc.).

About HF/HFI and its importance to SM

The guidance provides a summary of the five fundamental aspects of HF and HFI considered important for effective SM and demonstration that a system is safe to operate; these were:

- Designing out failure: ensuring that PSS are designed to be intuitive, easy to operate and tolerant to human failure (e.g. reduce opportunities for errors and violations and if errors do occur, ensure they are easy to detect and recover from)
- The human contribution to safety: explaining how humans can either positively or negatively contribute to safety
- Human failure: explaining the different types of error and violations that can lead to human failure
- Performance Shaping Factors: explaining how applying an understanding of psychology, physiology and sociology) can identify and elaborate on the aspects of work that influence human failure
- Human Based Safety Claims: outlining the importance of identifying and understanding the human based controls that reduce the potential for the hazard to occur and the likelihood of the hazard being realised, such as, performing a task in a certain way that helps to maintain safety (e.g. not flying an aircraft below a certain altitude) to responding to an emergency condition (e.g. a person in a control room identifies and responds correctly to an alarm).

Key best practice principles

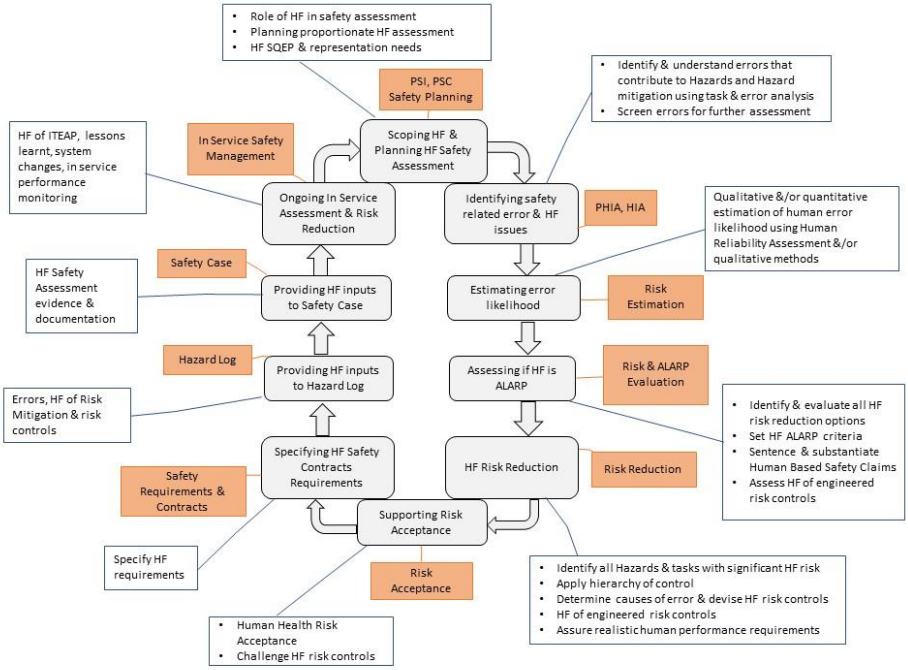
The guidance outlines around 20 best practice principles, summarised throughout the TG, aimed at both HF and SM specialists to help support more effective project-wide interactions

and to enhance and improve HF and SM integration. A selection of these is provided below.

- Conduct a scoping and proportionality review of HF based on the information available to the Project
- The Safety Management Plan and HFIP should be developed so they can be easily aligned (e.g. use the same method and terminology to indicate breakdown of work - what activities will be carried out, by whom and when)
- There is an expectation that some level of Task Analysis (TA) and associated error analysis will be carried out because of its importance in understanding human failure - justify if it has not been applied
- The decision to undertake further HF analysis walkthroughs, TA etc. should be a safety-led decision and informed by outputs from HAZID/HAZAN
- All safety claims made on people should be identified, defined and substantiated (e.g. demonstrates through argument and evidence that humans are capable of fulfilling the safety claim placed on them)
- HF specialists should be given the opportunity to review and challenge any outputs from Risk Acceptance, especially where HF measures have been adopted that place a claim on humans in the system.

Specific advice on how to integrate HF with the POSMS

As stated previously, the core content of the TG (e.g. advice and guidance to support the integration of HF with SM) was presented to align to the POSMS and the 13 POSMS SMPs – as shown in the diagram.



The POSMS SMPs describe the processes and procedures that are designed to assist with the identification and management of the safety risks of equipment and services throughout the acquisition process.

The guidance provided in the TG also used the same headings as the POSMS SMPs and these subsections in turn used the same standardised headings used by the POSMS SMPs. The purpose of structuring the guidance in this way was to help emphasise the link between HF and SM and to make the process of integration more straightforward and ensure consistency of language and terminology throughout.

For each section, a RACI (Responsible, Accountable, Consulted, Informed) table is provided, that outlines shared HF objectives for the POSMS SMP. An example RACI table is provided for SMP1 - Project Safety initiation is as follows:

	RACI Matrix			
PSI Objectives	**Responsible**	**Accountable**	**Consulted**	**Informed**
Appoint a person responsible for HF (the HFIF) within the DT.	*DTL*	*DTL*	*PSM*	*Other DT members*
Identify the key contacts and define roles and responsibilities.	*HFIF*	*DTL*	*PSM*	*Other DT members*
Understand HF within the programme through an initial scoping and proportionality review.	*HFIF*	*DTL*	*DTL, PSM, Other DT members*	*Other DT members*
Determine whether the HFIF is a Safety Management stakeholder and/or required on the PSC.	*PSM*	*DTL*	*HFIF*	*Other DT members*
Communicate the role of HF to the DT.	*HFIF*	*DTL*	*PSM*	*Other DT members*

Specific guidance is provided aligned to each objective; an example is provided below.

"The DTL has overall accountability for the consideration of HF within the Project and DT. In large Projects, or, Projects with a clear human element, the DTL should appoint a person to act as the HFIF, the person responsible for managing HFI contribution to safety particularly within the early stages of the programme (e.g. Pre-Concept and Concept). As the Project develops and evolves a Human Factor Integration Manager (HFIM) should be appointed to take on the additional work of ensuring that the contracted HFI Plan (HFIP) is implemented and to manage day to day HFI activities.

In smaller Projects, or during the pre-concept phase, the DTL may decide to act as the HFIF, however, as the Project develops it may be necessary for the DTL to delegate this responsibility to another DT member

The person responsible for HF at this stage of the Project (e.g. the person appointed as the HFIF) should support HF integration by:

- *Establishing points of contact and stakeholders;*
- *Engaging with the PSM;*
- *Understanding the Project and establishing the role of HF in Safety Management (e.g. scope, resource requirement etc.);*
- *Communicating the role of HF in Safety Management to the PSM to support stakeholder identification and PSC membership decisions;*
- *Developing an HF Strategy; and*
- *Developing Project awareness of HF e.g. the importance of considering the importance human contribution to safe and reliable operations)."*

Summary of HF analytic tools and methods that support Human Factors Integration (HFI) with System Safety

In addition to the specific advice, a series of tables is provided that provide a summary of Human Error Identification and Analysis methods as well as HF analytical tool and techniques that support SM. The methods and techniques are aligned to a category or area with a brief description of what they provide, a link to relevant POSMS SMP, an explanation of how they might be applied and references to additional guidance/information.

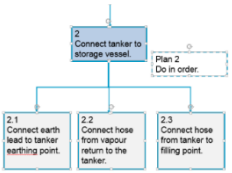
A small snapshot of 2 of the tables is provided below to illustrate the typical content.

Table 1: Human Error Identification and Human Error Analysis Techniques

Method	**Brief Method Description**	**Application to Safety Assessment**
Human Error Assessment and Reduction Technique (HEART) HEART – A Proposed Method for Assessing and Reducing Human Error. A Guide to Practical Human Reliability Assessment - This guide provides a practical overview of a range of Human Reliability Assessment methods, including APJ, PC, HEART and THERP.	HEART provides two tables: The first is a list of nine generic tasks allowing the assessor to select the task that most resembles the one being assessed. Each has a nominal human unreliability, e.g. 'Complex task requiring a high level of comprehension and skill' = 0.16 The second is a list of Error Producing Conditions (EPC), each of which has an associated figure that may be applied to modify the nominal human unreliability, e.g. 'A low signal-noise ratio' with a maximum assessed proportional of effect = 10. Using a simple mathematical formula, the method allows for multiple EPCs to be applied to each task, and for the proportion of effect of each EPC to be adjusted, thus leading to the final predicted HEP. HEART also provides suggestions for means of reducing error likelihood.	Supports quantitative Risk Estimation and derivation of HEPs. HRA also supports qualitative Risk Estimation.
Technique for Human Error Rate prediction	THERP is a means of quantifying HEP. The THERP manual (NUREG/CR-1278) provides tables, each with a set of HEPs which can be	Supports quantitative Risk Estimation and derivation of HEPs. HRA also supports

Method	Brief Method Description	Application to Safety Assessment
(THERP) Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. A Guide to Practical Human Reliability Assessment.	modified by the assessor to reflect the impact of PSFs (known as Error Factors), addressing errors of omission, commission and diagnosis of abnormal events. THERP manual Table 20-12 item 9: 'Set a rotary control to an incorrect setting', HEP = 0.001, Error Factor = 10 The method is suitable for use with fault and event trees, thus allowing detailed modelling of human failures. Unlike other methods, it can also account for dependency between related errors (see Human Error Inter-Dependence below) and can provide HEPS for error-recovery paths.	qualitative Risk Estimation.

Table 2: HF Tools and Techniques

Method	Brief Method Description	Application to Safety Assessment
Hierarchical Task Analysis (HTA) A Guide to Task Analysis. A Practical Guide for Engineering and Design.	HTA provides a graphical representation of a goal-based scenario broken down into tasks and sub tasks (operator activities required to achieve the goal). The sub tasks-are arranged in hierarchical levels of detail.  HTA is one of the most commonly applied HF techniques. HTA as with other forms of TA should be based on how work is actually carried out and should not just rely on procedures but use knowledge about how tasks are carried out from data gathering techniques such as walkthroughs etc.	Helps to improve understanding about how a task is carried out and what tasks are particularly dependent on people and therefore, potentially more vulnerable to error. Helps to show dependencies between tasks. HTA is frequently used in conjunction with TTA, to identify and better understand human failure.

Method	Brief Method Description	Application to Safety Assessment
Tabular Task Analysis (TTA) A Guide to Practical Human Reliability Assessment. A Practical Guide for Engineering and Design.	TTA is an approach that presents data (identified from TA, such as an HTA) in a tabular format to facilitate the identification and understanding of human failure. Each identified task is considered in detail to help identify and understand human failure. The approach to TTA is flexible but typically table columns would include: sub task, operator, potential errors (using a classification approach such as SHERPA), Consequence of the failure. Control measures to prevent against failure (e.g. safeguards); PSFs and recommendations (e.g. additional control measures or ways to enhance performance.	TTA is an important method used to identify and analyse errors in support of HAZID and HAZAN.

Recommendations

Recommendations were also made with the aim of enhancing HFI over and above provision of the TG. In summary these were:

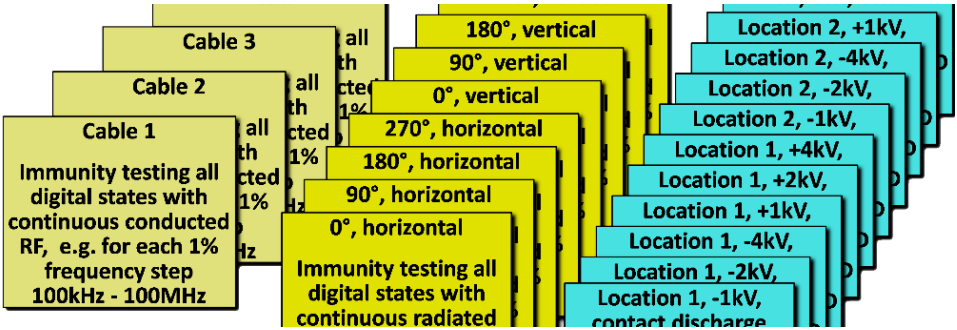
- Develop a suite of training courses to be delivered to both HF and SM specialists to provide comprehensive understanding of each other's role and methods and to build upon the information provided in the TG
- Provide greater Regulatory and Policy Over-Sight to encourage the integration of HF with SM, e.g. cite the TG in selected policy documents such as Joint Service Publication (JSP) 912 - Human Factors Integration for Defence Systems (V1.0 Oct 15)
- Conduct future research to identify, adapt, validate and if necessary, develop new HF safety assessment methods to meet the specific needs of the Defence sector
- Identify and capture case studies of good HF safety assessment in Defence and/or work examples that exemplify and disseminate good practice
- Enhance the suite of HF TGs to provide additional guidance on topics important to safety, such as, Error prevention and error risk reduction (e.g. preventing error interdependency).

David Pennie - Principal Consultant for Human Factors at Greenstreet Berman Ltd.

David has over 15 years' experience in the application of Ergonomics and Human Factors (HF) in high-hazard industries (e.g. defence, nuclear, rail & oil and gas). This experience includes consultancy (e.g. undertaking research, delivering training etc) but he also has extensive experience of providing embedded HF support working directly with both safety management specialists and engineers.

Copyright of this article remains with the author and is provided for subscribing SCSC members only and is not for further distribution without the express permission of the author.

Why do we need new standards for EMI Functional Safety Risks?



In this first of a series of articles focusing on Electromagnetic Interference (EMI), Keith Armstrong and Davy Pissoort discuss the challenges associated with managing EMI Functional Safety Risks and present the case for the need for further standardisation.

All electronics can be upset by electromagnetic (EM) disturbances, causing electromagnetic interference (EMI), so the functional safety risk management process should take EMI into account.

It is widely, but incorrectly thought that Electromagnetic Compatibility (EMC) testing covers everything that can go wrong, and all that is needed for managing Functional Safety is to increase immunity test levels to create a (*so-called*) "Safety Margin". This pervasive myth was debunked in 2004 [1] and again in [2], but it still seems to be very widespread, so it seems appropriate to reiterate why no amount of immunity testing can possibly demonstrate that a digital system has low-enough risks from EMI for typical Functional Safety applications, whatever the immunity test levels used.

"For at least 30 years it has been impossible to test more than a tiny fraction of all the possible digital states"

It is impossible to test all digital states even once

For at least 30 years it has been impossible to test more than a tiny fraction of all the possible digital states that a microprocessor and its software can get into, see [4] [5] [6] and [7]. We understand that, in 2013, the largest software companies in the world could only perform 100% state testing on printer drivers. Even with the fastest test system in the world, fully

testing many microprocessors or software programs would require millions, or possibly billions, of years.

Linear electronic systems can extrapolate from the results of testing a percentage of their possible states, to predict the behaviours of their untested states. But all digital systems are *non-linear*, which means that even if it was possible to test 90% of all their possible states (which it isn't), the results could never be extrapolated to predict the behaviour of the 10% that were not tested, see [8].

The digital industry has known for decades that their systems can fail in unpredictable ways as the direct result of untested combinations of *perfectly correct input*s, [9]. For example, if a digital system had four inputs, each digitized to 8-bit accuracy, plus 16 binary inputs (e.g. switches: either on or off), and if all inputs were independent of each other, there would be 2^{48} possible combinations of correct inputs, about $2.8 \cdot x\ 10^{14}$.

At 100 nanoseconds (ns) per input state test it would take $2.8 \cdot x\ 10^{7}$ seconds to test them all - about 326 days of testing 24/7, and of course, there are many more system states than are required for just the "input space", not least to handle the processing of the input data.

To discover whether EMI could cause an unsafe error or malfunction by immunity testing alone would require a large number of EMC tests to be applied in turn to all possible system states.

If we limit our example to the input space alone, when performing a radiated immunity test (e.g. to IEC 61000-4-3) the lowest frequency would be set at the correct level (taking measurement uncertainty into account), and the test would dwell at that frequency while the complete set of correct input states was exercised.

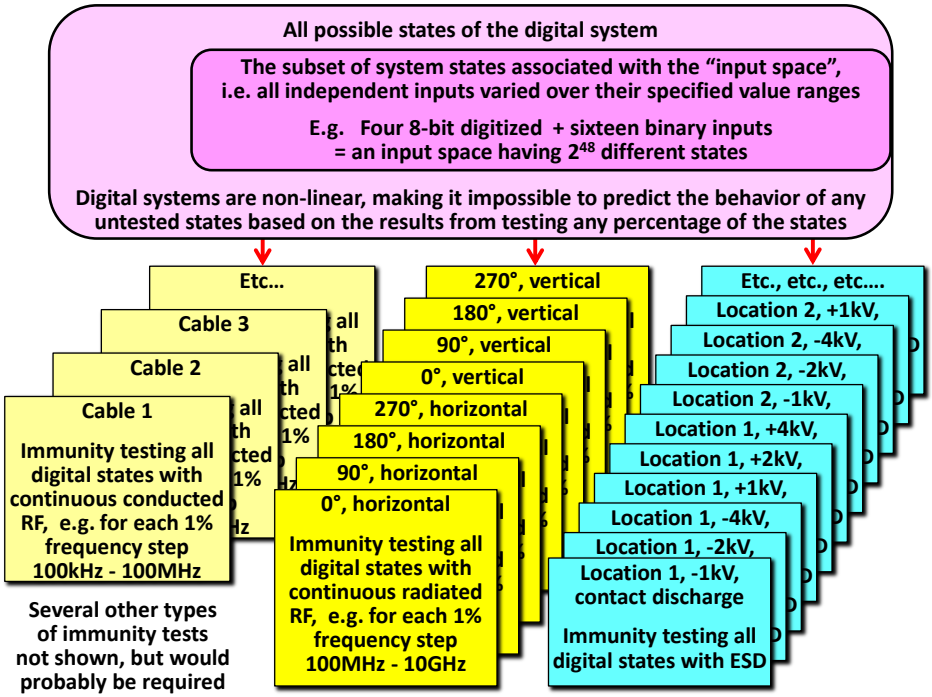
"A very simple immunity test plan would require a mere 5,000 years just to test the input state space"

For the simple example system above, this would take 326 days. Then the test frequency would be stepped 1% higher for another 326 days, and repeating this 230 times would cover the first *decade* of frequency (e.g. from 10 MHz to 100MHz), taking about 207 years of testing 24/7/365 to test just one decade of frequency with one angle of incidence and one antenna polarization!

Of course, this is all a gross simplification: it might be possible to reduce the testing time; and it might also be possible to speed up the testing of the system states. So let's assume that "intelligent" digital testing techniques reduce the number of states to be tested by 10 (without, of course, compromising the design confidence we need for SILs 1-4).

Let's also assume that each digital state can be tested in 1 ns instead of 100 ns. In this case, the very simple immunity test plan in the figure would require a mere 5,000 years just to test the input state space for this simple example system.

The idea of using immunity testing alone to prove a system is safe enough as regards EM disturbances, is clearly not viable.



Future mass-produced safety-related systems, such as those intended for autonomous cars, can be a lot more complex than the simple example shown. Assuming the DRIVE PX 2 [10] to have eighteen 8-bit digitized monochrome camera inputs, it would have 2144 possible input states, 296 times more than the simple worked example above.

The Near-Future EM Environment

The level of design confidence required for the desired SIL should be compared with the lack of confidence in knowing what the real-world EM environment of a system will be, over its entire lifecycle.

EMC immunity test standards, such as those listed under the European Union's EMC Directive, are claimed to cover 80-95% (depending on which standards' team member one talks to) of the typical daily/weekly EM disturbances in a typical application.

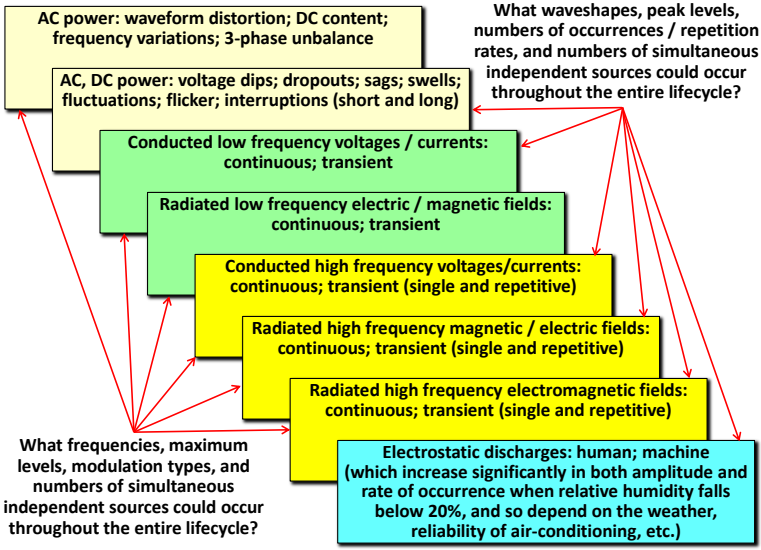
But even 95% confidence in setting a test level is a far cry from the 99.99% or better (for SIL1), required to help prove a system was safe enough. Also, these standards only cover typical daily/weekly EM disturbances, and ignore the effects of rare EM disturbances, even when they could be expected to occur during a typical lifecycle.

We also fail to understand why these test standards *still* do not cover the very close proximity (e.g. closer than 50mm) of cellphones and other personal electronic devices containing low-power radio transmitters, even though this is now a commonplace situation, and with the Internet of Things (IoT) will soon become ubiquitous.

In the next few years alone, the following general changes to EM environments are confidently expected:

- 5G cellphone systems with 100-times the data bandwidth of current benchmarks are expected to begin rolling out in 2020, but their frequency ranges, modulations and RF power levels, and how close the basestations will be to each other, are still unknown.
- Switching power converters will operate at frequencies 10 to 100 times faster due to the use of Silicon Carbide or Gallium Nitride devices, significantly reducing their size, cost and waste heat. This will in turn increase their use in many more applications, including all domestic appliances. Unfortunately, switching faster will also make them much noisier, at much higher frequencies.
- LED lighting will replace most incandescent and fluorescent lighting, using switching power converters that are much noisier than those technologies.
- Wireless Power Transfer (WPT) will use switching power converters to generate magnetic fields to charge the batteries in devices from cellphones to automobiles, trucks, buses, and trams at up to 22kW, with as much as 50% of these noisy fields "leaking" into the environment. Close proximity to WPT chargers will expose devices to intense fields, and it is impossible to ensure that this cannot happen.
- The use of PowerLine Telecommunications (PLT), sometimes called Broadband over PowerLine (BPL) is increasing, with ever-higher data rates.
- The use of Radio Frequency Identification (RFID) is increasing, with powerful fields generated near to their fixed or mobile readers.
- Machine-to-Machine (M2M) wireless data communications is expected to increase dramatically due to so-called Industry 4.0 and the IoT [11].
- Automobile safety systems will increasingly use steered radar beams of a few watts at frequencies including 76GHz, and modern silicon devices at 7nm or less are susceptible to such frequencies. Autonomous road vehicles may rely on several such radars, not just a single 'active cruise control' radar.
- AC electrical power networks will increasingly suffer harmonic and interharmonic waveform distortion/noise as linear loads continue to be replaced by non-linear loads such as the rectifiers in switching power converters. They will also suffer increasing levels of distortion due to the rapid increase in connections of AICs (active infeed converters), which convert the electrical power generated by photovoltaic panels/arrays, wind or water turbines, and other 'green' energy sources into a form suitable for feeding into mains power networks.
- Software-controlled radio will make better use of the limited radio spectrum by filling up any "empty" slots in the spectrum. The radio spectrum will eventually be entirely filled with frequency-hopping transmissions, for most of the time.

It is clear that even if immunity testing was practicable, it would be impossible to have any confidence in the types of EM disturbances or their test levels that should be used to be able to demonstrate that EMI should not cause unacceptably high risk levels during a lifecycle. The figure shows graphically, the problem of trying to predict the future EM environment with sufficient accuracy.



Real EM Environments are not simulated well-enough by EMC test standards

EMC test methods are designed for accuracy, repeatability, and low cost – and therefore do not necessarily simulate real life very well. For example, most radiated EM field immunity testing is done in anechoic chambers that create an environment unlike any real-life situation (other than an aircraft or missile in free flight). In real life there will be one or more surfaces reflecting EM fields from a variety of angles. The waveforms used for fast transient burst, surge and electrostatic discharge testing are very simplified versions of the real-world EM disturbances they are supposed to represent.

In some cases, the test waveforms are defined by what test equipment can be manufactured at an affordable price. For example, fast transient burst (FTB) testing uses pulses with fixed amplitudes and a repetition rate of either 5kHz or 100kHz, whereas, the EM disturbances from the electro-mechanical contacts that the FTB test is intended to represent actually varies in frequency from MHz to kHz as the contact gap opens, with a rising amplitude as the frequency decreases.

Another example is in electronic warfare and munitions where EMC experts know that when an RF 'threat' is modulated at a frequency corresponding to the rate of electrical activity in the target equipment, the target's susceptibility (vulnerability) increases dramatically.

Real-world sources of RF interference have a huge possible range of modulation frequencies, but normal immunity testing (using IEC/EN 61000-4-3 and IEC/EN 61000-4-6) uses only 1kHz sine-wave modulation, while military and some other standards use 1kHz pulse-modulation; neither of which is certain to discover all possible responses of the tested equipment to real-life RF threats.

One of the authors has been involved with two situations where equipment passed tests with any 1kHz sine-wave modulated radio frequency at up to 100 V/m, but were at least 80 dB more susceptible (i.e. would only take up to 10 millivolts/m) when the modulation frequency was set to their circuit's operating frequency. Both of these situations were discovered by accident, and both would cause severe financial and/or safety problems if interference occurred during normal operation.

Ref [12] makes the point that normal testing standards can give an erroneous impression of an equipment's EM performance in real life, due to the effects of load and temperature variations upon the inductors used in EMI filters; it gives an example of a mains supply filter's performance that fell by 20dB when operated at its rated maximum continuous voltage, current and temperature.

The Exploding EMC Test Plan

Assuming that all the issues discussed above have *somehow* been dealt with (although they cannot), the immunity tests would have to be performed many times to address the following real-life situations:

a) Reasonably foreseeable degradations and failures in EMC-significant components or connections (e.g. connector pins, solder joints, filter ground connections, etc.), throughout the lifecycle. These could be caused by: initial tolerances, aging, corrosion, use/misuse, wear, mis-assembly, temperature/pressure/humidity, vibration, shock, etc.

b) Foreseeable real-life EM disturbances in the system's intended operational environment that varied significantly enough from the traditional immunity tests (e.g. modulation type/frequency, transient waveshape and/or repetition rate, etc.) to warrant additional immunity tests.

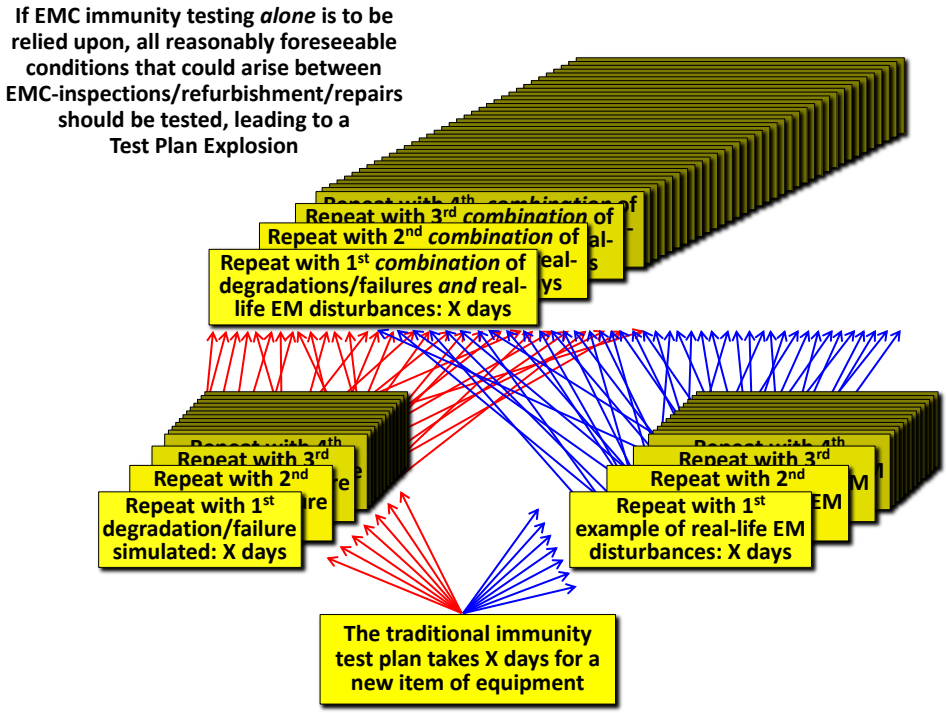
c) Foreseeable combinations of a) plus foreseeable combinations of b), during the lifecycle, for example:

- Two or more radiated fields at different frequencies
- A radiated field at any frequency plus an Electrostatic Discharge (ESD) event at any location and any voltage
- A radiated field at any frequency, plus a fast transient burst at any voltage
- A supply voltage at the low end of its tolerance plus harmonic distortion that reduces its peak height plus a dip, dropout or short interruption, etc.

Michel Mardiguian showed in [13] that when one EM disturbance is applied (e.g. a radiated RF field) the immunity of the equipment to another disturbance (e.g. fast transient bursts) can be seriously compromised. In his conclusions he stated:

"Speculating that all the worst EMI threats will appear at the same time on a given system would be extravagant. But relying on the belief that certain EMI combinations will never exist could be just as imprudent."

It very quickly becomes obvious that trying to cover all these reasonably foreseeable situations over the lifetime would create a "test plan explosion", as shown below.



Even if only 50 sets of tests were sufficient to simulate a), b) and c) respectively, this would require the immunity tests to be repeated 150 times. Few could afford to wait that long!

So, what are we to do about the functional safety risks that can be caused by EMI?

IET Standards published a Code of Practice on what it calls "Electromagnetic Resilience" in 2017 [14], and IEEE Standards is developing this further [3]. In the next article, "Management of Functional Safety Risks caused by Electromagnetic Interference" we provide further details of these publications and describe some current best practice techniques in managing EMI System Safety risks.

References

[1] K. Armstrong, "Why EMC Immunity Testing is Inadequate for Functional Safety," IEEE 2004 Int. Symp. EMC, Santa Clara, CA, August 9-13, ISBN: 0-7803-8443-1

[2] K. Armstrong, "Why increasing immunity test levels is not sufficient for high-reliability and critical equipment" IEEE 2009 Int. Symp. EMC, Austin, TX, Aug. 17-21, ISBN: 978-1-4244-4285-0

[3] IEEE Standards Association, project P1848, "Techniques and Measures to Manage Functional Safety

and Other Risks with Regard to Electromagnetic Disturbances", standards.ieee.org

[4] "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." from: "The Quality Attitude", Watts S. Humphrey, Carnegie Mellon University, November, 2009, on page 131 of resources.sei.cmu.edu/asset_files/SpecialReport/2009_003_001_15035.pdf.

[5] "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." An extract from: "A New Accident Model for Engineering Safer Systems," Professor Nancy Leveson, Massachusetts Institute of Technology (MIT), USA, "Safety Science," Vol. 42, No. 4, April 2004, pp. 237-270: sunnyday.mit.edu/accidents/safetyscience-single.pdf

[6] "We have looked at what it takes to validate autonomous driving, and the time needed was estimated at 100,000 years." Michael Bolle, in "Car safety and the digital dashboard" Chris Edwards, E&T Mag., 13 Oct. 2014, eandt.theiet.org/content/articles/2014/10/car-safety-and-the-digital-dashboard/

[7] "Building Robust Systems, an essay", G. J. Sussman, MIT, Feb. 23, 2008, groups.csail.mit.edu/mac/users/gjs/6.945/readings/robust-systems.pdf

[8] "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." from "Computer Based Safety-Critical Systems," The IET, September 2008 (this quotation does not appear in the 2013 edition)

[9] J. A. Whittaker, "What Is Software Testing and Why is it so Hard", IEEE Software, Jan-Feb 2000, pp 70-79 ieeexplore.ieee.org/document/819971

[10] "New DRIVE PX 2 Uses Deep Learning and Supercomputing to Enable Cars to Sense Surroundings, Navigate Autonomously", Jan 4, 2016, nvidianews.nvidia.com/news/nvidia-boosts-iq-of-self-driving-cars-with-world-s-first-in-car-artificial-intelligence-supercomputer

[11] D. Evans, "The Internet of Things. How the Next Evolution of the Internet Is Changing Everything", April 2011, www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[12] F Beck and J Sroka, "EMC Performance of Drive Application Under Real Load Condition", Schaffner EMV AG Application Note, 11th March 1999.

[13] M. Mardiguian, "Combined effects of several, simultaneous, EMI couplings", M. Mardiguian, 2000 IEEE Int. Symp. EMC, Washington D.C., ISBN 0-7803-5680-2, pp. 181-184.

[14] "Code of Practice on Electromagnetic Resilience", The IET, 2017, www.theiet.org/resources/standards/emr-cop.cfm

Keith Armstrong C.Eng, FIET, Senior MIEEE Cherry Clough Consultants Ltd, UK.

Keith graduated from Imperial College, London in 1972 with an Honours Degree in Electrical Engineering. He is a Fellow IET and Senior Member of IEEE, has chaired the IEE/IET Working Group on EMC and Functional Safety since 1997, and is UK's appointed expert to several IEC EMC standards committees.

Prof. Davy Pissoort, Senior MIEEE, Boydens Mechatronics Group.

Davy received his PhD degree in electrical engineering from Ghent University, Belgium in 2005 and worked as an R&D Engineer at Agilent Technologies (now Keysight Technologies) in Ghent. For the last 10 years he has been an associate professor and head of the Mechatronics Group at KU Leuven Bruges Campus.

Copyright of this article remains with the authors.

Risks caused by Electromagnetic Interference



Keith Armstrong and Davy Pissoort continue their discussion on the challenges in managing Functional Safety Risks posed by Electromagnetic Interference (EMI) and present current best practices in techniques and measures to manage the risks posed by EMI.

As introduced in the previous article, Electromagnetic interference (EMI) is what we call any errors, malfunctions or failures in electronics that are caused by Electromagnetic (EM) disturbances such as those listed below. Because all electronics can suffer EMI, it should be taken fully into account when complying with Functional Safety requirements.

Conducted low frequency phenomena	Harmonics, interharmonics Signalling voltages Voltage fluctuations Voltage dips and interruptions Voltage unbalance Power frequency variations Induced low frequency voltages d.c. in a.c. networks
Radiated low frequency field phenomena	Magnetic fields [a] Electrical fields
Conducted high frequency phenomena	Directly coupled or induced continuous voltages or currents Unidirectional transients [b] Oscillatory transients [b]
Radiated high frequency field phenomena	Magnetic fields Electrical fields Electromagnetic fields – continuous waves – transients [c]
Electrostatic discharge phenomena (ESD)	Human and machine
Phenomena of conducted and radiated HPEM environment [d]	
High altitude electromagnetic pulse (HEMP) [d]	

[a] Continuous or transients.

[b] Single or repetitive (bursts).

[c] Single or repetitive.

[d] To be considered in case of special conditions (see IEC 61000-2-13).

NOTE There is no abrupt change between the low frequency domain and the high frequency domain but a soft transition between 9 kHz and 150 kHz. For formal applications the limit is set at 9 kHz (scope of CISPR).

We understand that it is commonplace for Functional Safety projects to allocate one-tenth of the maximum acceptable risk level to EMI, unless there are specific reasons for choosing a different proportion. For example, if a Safety Related system (SRS) is required to maintain a risk of death of 1 in a million per person per year, then the risk of death arising from EMI effects must be less than one in ten million per person per year.

Immunity testing in an Electromagnetic Compatibility (EMC) laboratory is the traditional method of ensuring that EMI is sufficiently unlikely to occur during real life operation, and where safety risks are involved, it has been usual to apply the standard immunity tests at higher levels than otherwise. Although it is now more than 13 years since this approach was publicly revealed as being insufficient [1] [2], it is still used, and this continues to expose people to uncontrolled safety risks, and exposes manufacturers to uncontrolled financial and reputational risks. This is especially so because more advanced electronic systems are increasingly being used to control dangerous activities (e.g. remote-controlled surgical robots; care-giving robots; self-flying goods-delivery drones; autonomous cars, etc.).

"More advanced electronic systems are increasingly being used to control dangerous activities (e.g. remote-controlled surgical robots; care-giving robots; self-flying goods-delivery drones; autonomous cars)"

There is a simple reason why immunity testing is insufficient in proving that EM disturbances should not cause unacceptable levels of functional safety risks: it is physically impossible to test all of the possible states of a modern, programmable SRS.

Even if it *was* possible to test all possible digital states (*which it isn't*), there are additional cost and time barriers to relying solely on immunity testing (discussed in detail in [3]). This makes it obvious that attempting to use immunity testing alone to prove that functional safety risks due to EMI would remain low-enough throughout a lifecycle would cause an 'explosion' in the cost and duration of an EMC test plan [3] [1].

'High-spec', well-maintained EM mitigation (shielding, filtering, surge protection, galvanic isolation, etc.) has long been the traditional military method for reducing risks that could be caused by foreseeable EM disturbances over a lifecycle. Some examples are shown in the figure. It reduces the levels of EM disturbances to which the electronics are exposed to such low levels that EMI cannot occur. Such mitigation is ruggedized so as to maintain its high EM specifications between maintenance and/or refurbishment periods and is over-engineered to cope with the uncertainties in predicting the EM disturbances that could arise.

The large size, weight and/or cost of the ruggedized 'high-spec' EM mitigation approach does not suit many modern SRSs, so the IET's Working Group on EMC for Functional Safety developed a practical alternative based on the expertise that existed in both the EMC and Functional Safety professional communities. After considerable input from a large number of these experts in the UK, the IET first published this guidance in August 2013 [4].



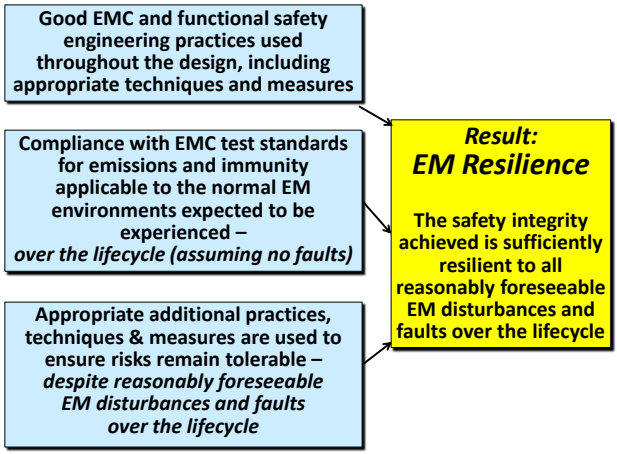
Since then, the IET's WG has revised this guidance, put it through two international commenting rounds and published the result in 2017 as the IET's 'Code of Practice on EM Resilience' [5]. The figure on the next page provides an overview of this 'EM Resilience' approach, which essentially means that the hardware and software could suffer from EMI without causing unacceptable levels of risk.

The draft new IEEE Standard 1848 [6] is a direct development of [5].

IEC 61508 describes many Techniques and Measures (T&Ms) for use in specification, design, verification and validation; for hardware, software and systems. Firstly, to try to prevent avoid errors, malfunctions and faults from occurring, and secondly to reduce any remaining risks to conform to the specified risk levels.

These T&Ms operate on the data and other signals (analogue, digital, etc.) and/or on the electrical power supplies (AC, DC, etc.), but they were never intended to deal with EMI. However, EMI can only affect data, signals and/or power supplies, so it is commonly found that correct application of IEC 61508's T&Ms is very effective in dealing with the effects of EMI. Functional safety designers and their assessors have become very experienced in the use of these T&Ms.

The IET's 2017 guidance [5] provides guidance on how best to apply IEC 61000-1-2:2016 in practice. It details which of IEC 61508's T&Ms are good for dealing with EMI, as well as how to improve their benefits for EM resilience, and includes a few new T&Ms specifically for dealing with the effects of EMI. These modifications do not require functional safety designers or their assessors to learn very much more beyond their knowledge of the existing standards.



EM Resilience T&Ms in design

Electronic hardware, software and system designers are generally familiar with many of these T&Ms, because most of them have been in use for decades.

T&Ms for Redundancy and Diversity include:

- Multiple sensors sensing the same parameters
- Multiple communications carrying the same data
- Storing multiple copies of data
- Processing the same data with multiple processors
- Detecting errors by comparing one value with another, out of any multiple of values
- Correcting errors, for example by 'voting' any two that agree out of three, or three out of five, etc.

All the above benefit from using a wide range of diverse technologies and techniques among their multiple "channels" to improve their effectiveness against the common-cause failures typically caused by EMI. For example, in a system consisting of two identical channels, the signals or data in one channel could be inverted thereby making EMI more likely to be detected when comparing the difference between their outputs, at no extra cost.

T&Ms for Error Detection & Correction include:

- Error detection coding (EDC)
- Error correction coding (ECC)
- Static self-testing checks the hardware and software before operation, preventing start-up if necessary

- Dynamic self-testing checks that the operation of the hardware and software is correct during operation, for example by regularly inputting fixed, known signals/data and checking that the resulting outputs are within the required boundaries. Critical aspects of data processing might be checked for correct operation once every second, or perhaps even more often.

T&Ms for Power Supplies include:

- Window comparators check that power supplies are within design limits.
- Stored energy (e.g. batteries, supercapacitors) used when external power supplies are outside design limits. This is a very common technique used in modern portable devices, such as cell phones or tablet PCs, and the technology is very well-developed as a result.
- Multiple power sources (whether external or internal storage) operated in parallel (e.g., so-called N+1 redundancy) so that the failure of one or more power sources still allows normal operation to continue.
- Before all the available sources of power fail, the system switches to a safe state (if it has one). If it doesn't have one, more energy storage or more redundancy in external supplies is added until the possibility of dangerous failure is as low as required.

Choosing T&Ms for EM Resilience will generally discover that many of the necessary T&Ms have already been chosen for other Functional Safety reasons. However, many of these will need to be modified as described in [5] to optimise their benefits for EM Resilience. Other EM Resilience T&Ms may then need to be added to achieve EM Resilience overall.

In a system, some items of equipment or elements may rely on military-style high-spec mitigation; whilst other may rely on EM Resilience T&Ms.

It is possible to create functionally safe systems by relying solely on IEC 61508's design T&Ms to detect failures and switch the Equipment Under Control (EUC) into a safe state. However, EMI can make them fail to start up, or switch to their safe states much too frequently.

Such systems should be expected to be modified by their users or owners to improve their 'availability' (reduce their downtime) usually by disabling their SRSs, see sections 3.8 and 3.10 in [7]. In the EU at least, product liability laws would seem to categorize such unauthorized modifications as 'foreseeable misuse', making it the *manufacturer's* fault if any deaths, injuries or financial losses resulted from users disabling SRSs to improve an EUC's availability.

As far as EMI is concerned, adequate availability simply requires compliance with the normal relevant EMC immunity test standards. These include immunity test standards that have been used for decades for compliance with the EMC Directive, and customers' EMC specifications for railway signalling, automobiles, military equipment, avionics, etc.

The EMC testing community has extensive experience with ensuring that equipment passes EMC tests when it is shiny and new. The IET's 2017 guide [5] recommends that SRSs maintain their ability to pass all relevant EMC tests *throughout their entire lifecycles.* This should not require competent EMC designers to have to learn a great deal more.

T&Ms for verification and validation

Suitable verification and validation methods include (but are not limited to):

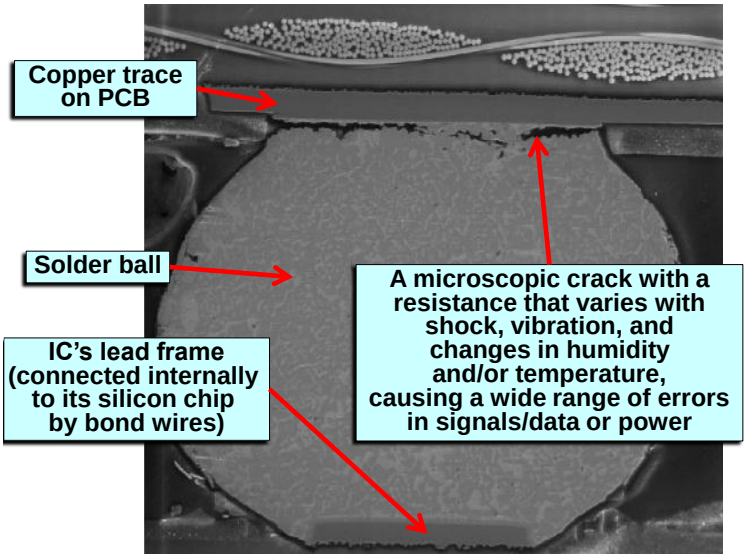
- Demonstrations
- Checklists
- Inspections
- Walk-throughs
- Reviews
- Assessments
- Audits.

Each of these can use one or more of the following analysis techniques:

- Inductive
- Deductive
- "Brainstorming"
- Validated computer modelling
- Testing.

Functional Safety designers and their assessors have become very skilled with using these methods, *but they were never designed to deal with EMI*. To help achieve EM Resilience, they should be competently modified or extended.

A good example is the solder joint as shown below:



Clearly, slight movements due (for example) to changes in temperature and humidity can cause the resistance of this solder joint to vary over a wide range, and vibration can modulate the value of its resistance causing what is sometimes called "mechanically induced EMI."

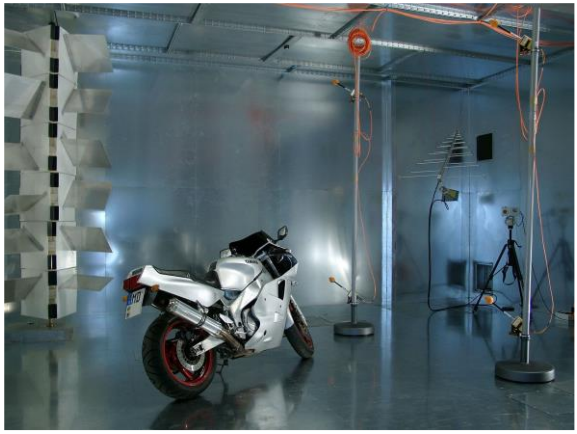
For these reasons, [5] and [6] recommend that all verification and validation techniques be competently modified to take full account of EMI. In particular, they need to take account of the following facts peculiar to EM disturbances:

- EMI can cause one or more signals, data and/or controls to suffer from an almost infinite variety of degraded, distorted, delayed, re-prioritized, intermittent and/or false values
- EMI can cause one or more power supplies to suffer from an almost infinite variety of waveform distortions, overvoltages, undervoltages (dips, dropouts, interruptions, etc.)
- The above EMI effects can all happen simultaneously (i.e. everything can go wrong at once, in any number of different ways), or they can happen in any time sequence that could have critical safety consequences.

A wide variety of test methods has been developed over many decades to help prove that hardware and/or software will be sufficiently reliable, and these should be used wherever appropriate, taking into account both the application and the acceptable level of Functional Safety risk.

Techniques similar to HALT (Highly-Accelerated Life Testing) are also recommended to help prove that the physical implementation will be reliable enough over the entire lifecycle, including mechanical structures, electrical connections, printed circuit boards, solder joints, etc., to help ensure that the SRS will remain compliant with all relevant immunity test standards over its entire lifecycle, as mentioned previously.

There are significant benefits to be had by extending the standardized EMC tests, and by adding non-standardized EMC tests/checks, to help verify and validate that the EM resilience is sufficient. For example, standard immunity tests can be extended by using (see [8], [9]):



- Increased frequency ranges, both lower and higher
- Higher test levels
- More angles/polarizations in radiated testing, e.g., by using reverberation chamber testing as shown in the figure opposite
- Frequencies that a design is especially susceptible to, stimulated by the carrier frequencies themselves, or by demodulation or intermodulation [10]

During any immunity testing, all variations in functional performance should be recorded and analysed afterwards to see if they could have any possible relevance for the Functional Safety risks of the final SRS. This is especially important when EMC laboratory testing is only performed on individual sub-systems, and not on the final SRS as installed.

For example, a fast transient burst might cause a DC power converter to shut down for a second or two to protect itself from damage, which might be perfectly acceptable *in the context of the power converter unit itself, alone*. But when it is powering a microprocessor that must continue to operate correctly to ensure Functional Safety, the time the processor takes to reboot after such a power interruption might not maintain acceptable safety risk levels. This simple example shows that what is acceptable for an individual element of an SRS, might be completely unacceptable for that SRS as a whole. Careful and competent post-testing analysis is therefore necessary.

A useful verification and validation T&M for EM resilience is to repeat the standard or extended immunity tests on units during and after accelerated aging to simulate the effects of the foreseeable physical, climatic and user environments over the lifecycle.

Many manufacturers build two prototypes, one of which goes for HALT testing and one for EMC testing. But they generally don't take a HALT tested (but operational) unit and quickly

recheck its immunity, to see if its EM mitigation needs to be more robust, or if a planned maintenance schedule is necessary to ensure that EMC compliance is maintained throughout the lifecycle.

More information on T&Ms for EMI resilience is given in [11], and [5] [6] provide more detail.

Conclusions

EMC immunity testing alone cannot ensure acceptable Functional Safety risks, however high the test levels used [1] [2]. The only practical techniques that we know of at the time of writing, which can be used to demonstrate that EM disturbances will not cause Functional Safety risks to exceed acceptable levels are:

- The ruggedized high-specification well-maintained EM mitigation 'military' approach
- The "EM Resilience" approach, which applies a suitable combination of techniques and measures as described in the IET's 2017 guide [5] and the forthcoming IEEE Standard 1848 [6]. Other T&Ms that provide the same resilience for all foreseeable EM disturbances may be used instead.

EM Resilience is too new to be able to describe case studies, but because its methodology is based on small and rather obvious extensions to what Functional Safety and EMC engineers have been doing very successfully for more than two decades, no great difficulties are anticipated.

References

[1] K. Armstrong, "Why EMC Immunity Testing is Inadequate for Functional Safety", IEEE 2004 Int. EMC Symp. Santa Clara, CA, August 9-13, ISBN: 0-7803-8444-X

[2] K. Armstrong, "Why increasing immunity test levels is not sufficient for high-reliability and critical equipment", IEEE 2009 Int. Symp. EMC, Austin, TX, August 17-21, ISBN: 978-1-4244-4285-0

[3] K. Armstrong, "Why Do We Need an IEEE EMC Standard on Managing Risks?" 2016 IEEE EMC Magazine – Volume 5 – Quarter 1, ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7477140

[4] "Overview of techniques and measures related to EMC for Functional Safety", The IET, 2013, www.theiet.org/factfiles/emc/emc-overview.cfm

[5] "Code of Practice on Electromagnetic Resilience", The IET, 2017, www.theiet.org/resources/standards/emr-cop.cfm

[6] IEEE Standards Association, project P1848, "Techniques and Measures to Manage Functional Safety and Other Risks with Regard to Electromagnetic Disturbances", standards.ieee.org/

[7] Yuvin Chinniah, "Analysis and prevention of serious and fatal accidents related to moving parts of machinery", Safety Science 75 (2015) 163-173, www.elsevier.com/locate/ssci

[8] K. Armstrong, "Testing for immunity to simultaneous disturbances and similar issues for risk managing EMC", IEEE 2012 Int. Symp. EMC, Pittsburgh, PA, August 5-10, ISBN: 978-1-4673-2059-7

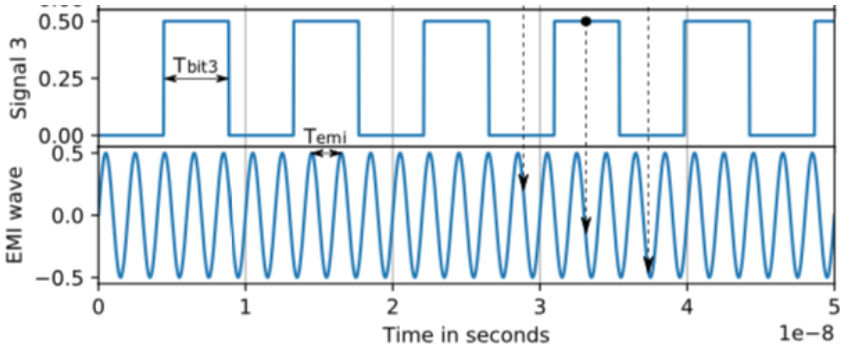
[9] W. Radasky and K. Armstrong, "Non-Standardized Immunity Test Techniques to Help Manage Risks caused by EM Disturbances", IEEE 2016 Int. EMC Symp., Ottawa, Canada, July 2016, ISBN: 978-1-5090-1441-5 (USB) or 978-1-5090-1439-2 (CD-ROM)

[10] Dipl. Ing. (FH) W. Grommes and K. Armstrong, "Developing Immunity Testing to Cover Intermodulation", IEEE 2011 Int. EMC Symp., Long Beach, CA, August 15-19, ISBN: 978-1-45770810-7

[11] J. Silberberg and K. Armstrong, "EMC Risk Management", half-day workshop, IEEE 2015 Symp. EMC&SI, Santa Clara, CA, March 15-21, ISBN: 978-1-4799-1991

Copyright of this article remains with the authors.

Hardware and Software Techniques and Measures to Effectively Manage EMI Functional Safety Risks



Keith Armstrong, Davy Pissoort and colleagues discuss the effectiveness of different hardware and software based techniques and measures used to reduce risks related to electromagnetic disturbances in mission- or safety-critical systems.

Concerns about the possibly serious consequences of Electromagnetic Interference (EMI) in mission- and safety-critical applications started about two decades ago. At first, the general belief was that all that was needed was a more solid application of the classical "hardware-only" EMI mitigation (i.e. grounding, filtering, shielding, etc.) combined with more severe testing (i.e. increased test levels). However, recent literature [1]-[3] has shown that no feasible and economically affordable EMI test plan can ever prove the high (equivalent) mean-time-to-dangerous-failures required within mission- or safety-critical applications. Indeed, an enormous amount of testing (i.e. multiple decades of continuous testing) would be required to duplicate all possible combinations of the many simultaneous types of EMI that an electronic system may encounter over its lifetime in its operational environment, while also covering all possible states of both hardware and software. Because digital systems are non-linear, no subset of testing can prove that the whole is safe and/or dependable enough.

More recently [4], insight has grown and indicates that the only cost-effective approach is the one in which the classical EMI mitigation techniques are complemented with a thorough EMI risk analysis, as well as appropriate risk reduction techniques and measures (T&Ms) that are typical in the discipline of Functional Safety. These T&Ms can be applied both in hardware as well as in software. The aim is to develop systems that are inherently resilient

to EMI. In case of disturbance, the applied T&Ms should make the system fault-tolerant for EMI so that the system either continues to work as intended in a safe manner or switches itself into a safe-state. This approach is described in general terms in the IET Code of Practice on EMI for Electromagnetic Resilience [4][5] and is also included in the IEEE Standard on Managing Risk due to EMI [6]. Although IEC 61508, the mother standard on Functional Safety, describes a broad set of T&Ms that over the years have become well understood, well-proven and widely used, these T&Ms were not originally developed to deal with EMI, nor were they ever studied in detail with respect to EMI. As EMI has become a major safety concern, these T&Ms need to be improved and adapted such that they effectively cope with EMI.

Hardware based T&Ms: Electromagnetic (EM) Diverse Redundancy

A typical T&M applied for mission- or safety-critical functions is to have two or more identical sets of hardware and software with the same inputs and performing the same operations on them. A few examples are:

- Multiple sensors sensing the same parameters
- Multiple copies of data stored
- Multiple communication channels carrying the same data
- Multiple processors processing the same data.

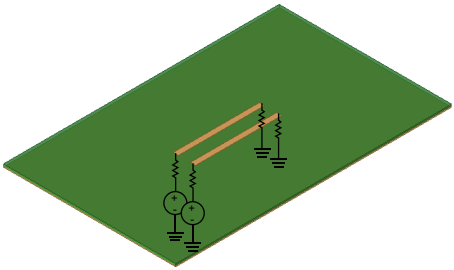
When a malfunction occurs in one of these 'parallel channels', a comparator/voter detects that their outputs no longer agree and triggers appropriate actions to maintain safety. Unfortunately, the malfunctions that EMI creates in identical channels can easily be so similar that the comparator/voter cannot tell that there was a problem at all. To be effective against EMI, the parallel paths should exhibit a different behaviour when subjected to the same EMI ("EM-diversity"). Options include, but are not limited to:

- Inversion of data on otherwise identical channels
- Spatial diversity where the placement of the parallel channels is chosen such that the likeliness of being disturbed by exactly the same EMI is reduced
- Time redundancy where the parallel channels work in different time windows
- Frequency redundancy where the parallel channels work at different frequencies.

The effectiveness of these four types of EM diversity is studied in more detail below, for the case where the EMI comprises a strong, continuous EM field ("plane wave)". To get statistically meaningful results, a very large set of plane-waves is considered, with each of the plane-waves having a random angle-of-incidence, polarization and phase.

Effectiveness of inversion

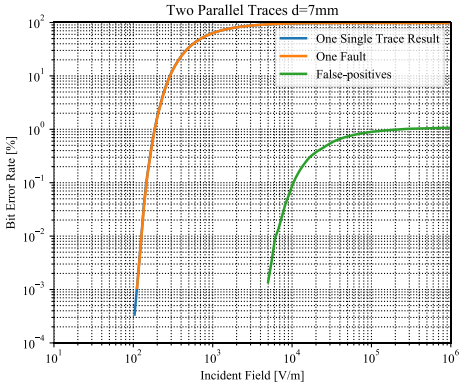
The figure shows the geometry considered for the study of the effectiveness of inversion [7]. It comprises a two-channel redundant system formed by two parallel traces on a simple Printed Circuit Board (PCB). The PCB is an FR4 substrate of 10cm by 16cm and 1.6mm thickness. All traces have a width of 3mm and a length of 5cm. The

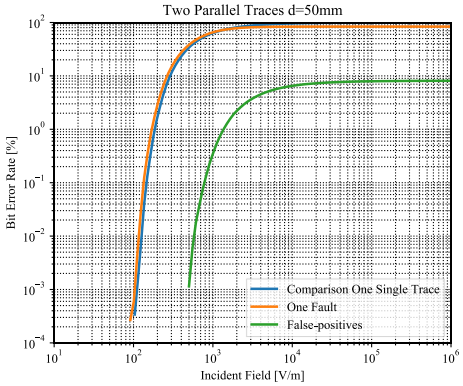


traces are terminated in 50 Ohm loads, i.e. the characteristic impedance of the traces, at both ends. Over the traces, a large random set of bits is transmitted from one end to the other of each trace. At the same time, the PCB is disturbed with a strong continuous EM field ("plane wave)", as explained above.

For the encoding and decoding, Unipolar Non-Return-to-Zero-Level was used, with the following metrics. For encoding, the voltage levels for a '0' and a '1' at an input sides of the traces are 0V and 1V, respectively. For the decoding, the thresholds used to differentiate between a '0' or a '1' are set to 1/3rd and 2/3^{rds} of the theoretical output voltage, respectively. If the voltage is below the 1/3rd threshold, then a '0' is seen. The same goes when the voltage is above the 2/3^{rds} threshold, at which moment a '1' will be read. For any values in between the thresholds, the bit is seen as faulty, to create a worst-case result. For easier processing, a decoding technique is used where we don't look at the transient behaviour of the received bit patterns, but only at the middle of each received bit. So, our analysis does not use any special detection techniques (eg. Schmitt-trigger). The Bit-Error-Rate (BER) is used as the metric to assess the effectiveness of inversion. The BER is defined as the ratio between the number or bits that are decoded incorrectly at the output side versus the total number of bits that were considered.

With inversion, the bit patterns on the two traces are opposite to each other. This means that on one trace a '1' is represented by a high voltage, while on the other a '1' is represented by a low voltage. At the end of the two traces an ideal voter is assumed. This voter compares the bit patterns of both traces. If at one moment in time, the received bits at the end of the two traces are not the same (taking into account that for one trace these were inverted), then the voter flags that an error must have occurred and can trigger that the Equipment Under Control (EUC) puts itself into a safe-state. However, dangerous failures can occur when both bits at the end of the traces are wrong at the same time ('false positive'). In that case, the voter would assume wrongly that there is no error at all, and would not trigger the EUC to put itself into a safe-state and would continue with the wrong data. Such a "two faults"-situation or "false-positive" can happen when the induced voltages on the two microstrips have a phase difference that is sufficiently large. In that case, the induced voltage can cause both decoded bits to be wrong. Another possibility is that the induced voltages levels fall between the thresholds, so that the decoder also detects a faulty bit (a voltage level between both thresholds was always considered faulty in this study). The probability





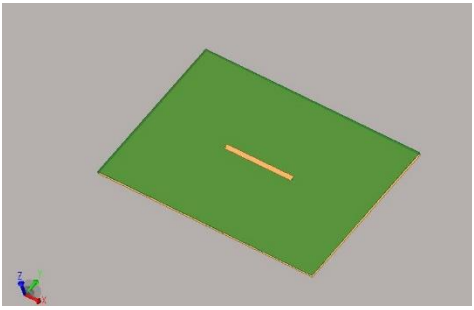
that this happens becomes greater with increasing distance between the traces. The figures on the previous page illustrate this for a bit frequency of 200MHz and a disturbance frequency of 500MHz respectively. Hence, for inversion to work properly, both traces should be completely identical and as close as possible to each other.

Effectiveness of spatial diversity

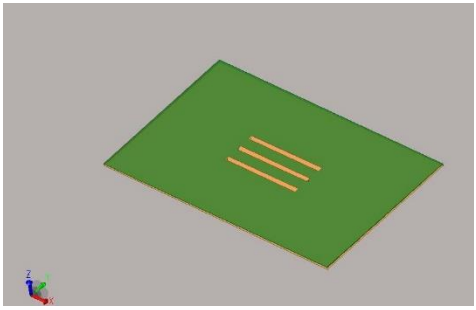
To study the effectiveness of spatial diversity [8][9], four different geometries have been considered:

- A single PCB with a single trace (top left figure). This is the reference situation (non-redundant system)
- A single PCB with three parallel, identical traces (6mm spacing between the traces) (top right)
- A single PCB with three identical, but differently oriented traces (bottom left)
- Three identical, but differently oriented PCBs (bottom right)

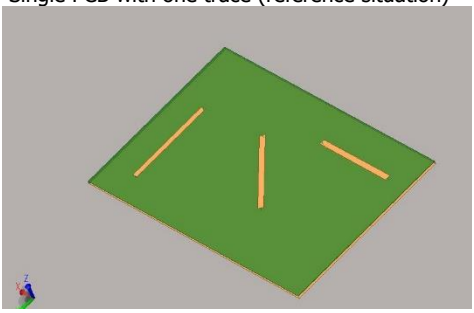
All of the redundant systems are 2oo3 systems. This means that after the (ideal) voter, a bit error will only occur if the bit error occurs for at least 2 of the redundant paths. Note that there is a significant difference with respect to what can be obtained with a 2oo3 system compared to a 2-channel redundant system as studied in the previous section on inversion. Indeed, with a 2oo3 system one can use majority voting to obtain fault-tolerant behaviour. In contrast, with a 2-channel system, one can only detect that an error has occurred (when both channels have a different outcome) upon which one can trigger an appropriate action (e.g. transition to a fail-safe state).



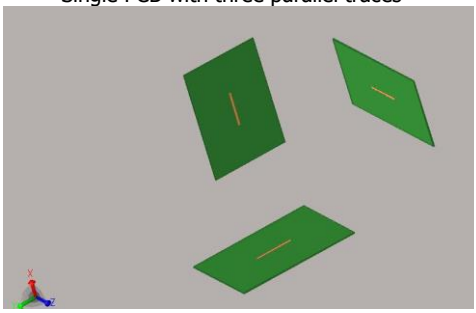
Single PCB with one trace (reference situation)



Single PCB with three parallel traces

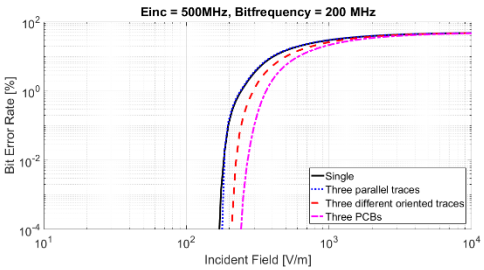


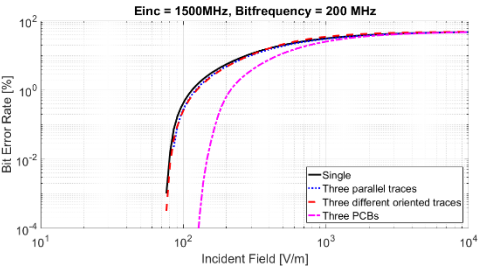
Single PCB with three differently oriented traces

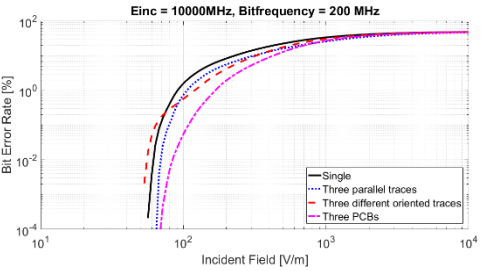


Three differently oriented PCBs

The resulting BER (i.e. after the ideal voting) vs the amplitude of the incident field is shown in the following figures for a disturbance at 500MHz, 1.5GHz, and 10GHz, respectively. In all cases, the bit frequency is 200 MHz.



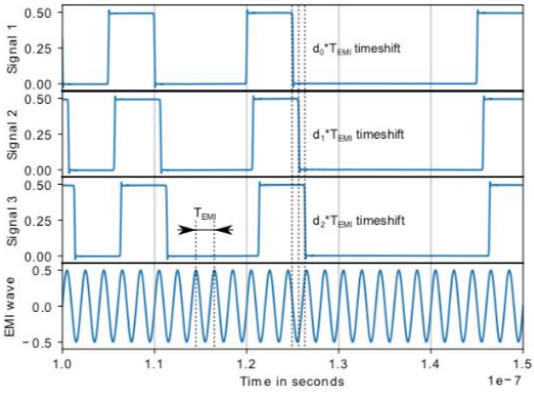




As expected, the situation with the redundant system comprising only a single PCB with three parallel traces doesn't give much benefit compared to the non-redundant system. Only when the frequency goes up such that the distance between the traces becomes "electrically" large, the BER of the situation with three parallel traces behaves (slightly) better than the non-redundant system.

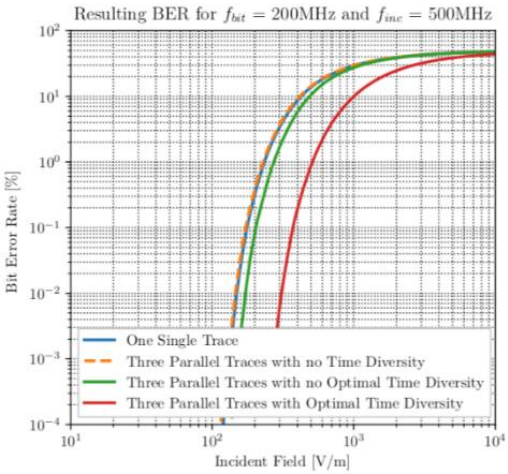
The single PCB with three differently oriented traces behaves somewhat better at some of the frequencies. However, at other frequencies, its benefit is only limited or even worse compared to the single trace. A possible cause might be that two of the three paths are located more closely to the edge of the PCB where they are more sensitive to an incoming plane wave. Only the case of three different PCBs results in a consistent reduction of the BER.

Effectiveness of time diversity



In this situation, the diversity property is created by changing the timing according to the redundant channel data being transmitted [10]. The reasoning behind time diversity is that the data is sampled at a constant rate (the bit frequency), and that point in time never changes. This means that for all three redundant channels, where the voltage induced because of EMI is nearly the same, the sampled value will be nearly the same every time. If we could change that point in time where the three different channels are sampled, a different value from the disturbance will be sampled, and this would create a straightforward EM-diverse system. This principle is shown in the figure above where the timeshift is represented by a percentage of the period of the frequency of the disturbance.

The following figure shows the BER in function of the strength of the EMI disturbance for a non-redundant system and a 2oo3 system (parallel traces as shown earlier) with and without the application of time diversity. Once again, the disturbance frequency was 500 MHz and the bit frequency 200 MHz. It is seen that the performance of time diversity heavily depends on the timeshift.



A quite brute-force method was used to find out what combination of timeshifts is the most optimal. This was done by creating a long list of random bits, and encoding them to voltages. A sine-wave with the desired EMI frequency is used to simulate the incoming disturbance.

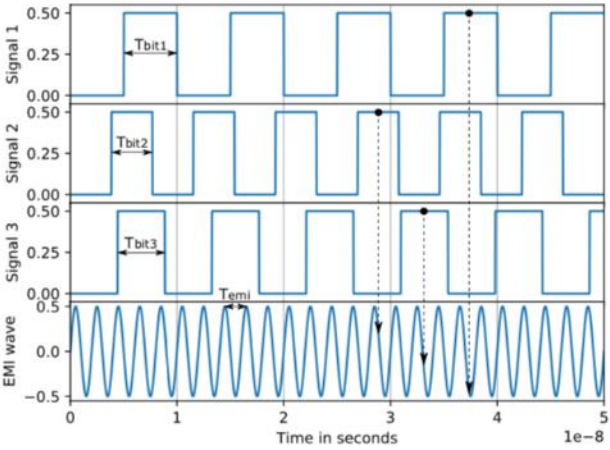
The time delay between the bit patterns is swept for two of the three trace inputs, one input is fixed at 0% or no time delay. The profile of the sweep is from 0%-40% of the period of the bit-frequency, which is equal to 0%-100% of the period of the EMI frequency. The results of this study showed that for a 2oo3 system, a timeshift of 0, 1/3 and 2/3 times the period of the incoming EMI disturbance has the best performance. When we look at a sinewave and take three sample points that are shifted 120° at all times, one notices that those points are the most different when comparing to other combinations of timeshifts.

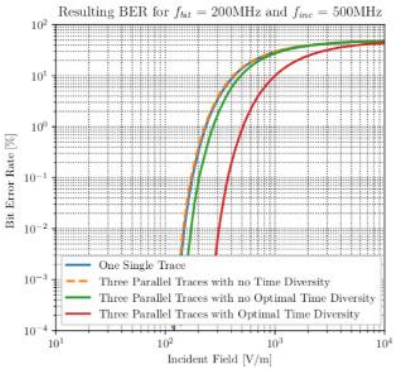
It was confirmed that these results can be extrapolated to more general NooM systems. For example, for a 3oo5 system, the optimum timeshift is 1/5th of the period of the EMI disturbance.

Effectiveness of frequency diversity

The goal of frequency diversity is to use three different frequencies for the data transmission.

This will change the position in time where the bits will be sampled at the output, and thus change the value of the induced voltage that will be measured by the output as shown in the figure opposite.





The figure shows the BER in function of the strength of the EMI disturbance for a non-redundant system and a 2oo3 system (parallel traces as shown earlier) with and without the application of frequency diversity. Once again, the disturbance frequency was 500 MHz. It is seen that the performance of frequency diversity heavily depends on the choice of the three frequencies f_1, f_2 and f_3. It can be proven (but the mathematical analysis falls outside of the scope of this contribution) that an ideal combination is (assuming that f_1 is given and that the frequency f_{EMI} of the disturbance is known): f_1, $f_2 = f_1 + f_{EMI}/3$, and $f_3 = f_1 + 2f_{EMI}/3$.

Software based T&Ms: Error Detection and Correction Codes

In order to protect communication channels from bit errors, Error Detection and Correction Codes (EDCCs) have been developed and used since the 1950s. Such EDCCs add redundant information (bits) to the actual data in order to enable the receiver to detect or even correct corrupted information. Cyclic Redundancy Checks (CRC), Hamming Codes and Data Triple Modular Redundancy (TMR), also called Triplication, are well known examples. Below, we discuss the effectiveness of these codes to cope with strong, continuous EMI disturbances. An important concern is whether or not false negatives can occur, i.e. whether corrupted and, hence, incorrect data could be seen as correct.

In all sections below, the geometry under study is the PCB with a single trace – the reference situation discussed earlier. At the input side of the trace, a data producer generates data words, encodes them (either with or without an EDCC) and puts these code words onto the communication channel (the PCB trace in this case). The channel then transmits the code words to the data consumer at the output side of the trace. The data consumer decodes the received code words to data words. The entire communication subsystem is subjected to a continuous EMI disturbance. In order to check the effectiveness of the considered EDCCs, the decoded data word is compared to the original data word that was sent.

Cyclic Redundancy Checks (CRC)

A data word is initialized at the data producer, and its CRC [11] is calculated and added to the data word before sending all bits over the communication. The CRC is in essence the remainder after a bit-wise division. Both the sender and receiver use the same divisor, called the polynomial. In this study, data words consisted of 32-bits, whereby the first 16 bits are data and the second 16 bits are its CRC value. For the 16-bit CRC-CCITT method, the following divisor is used: $x^{16} + x^{12} + x^5 + 1$. At the receiver side, the data consumer, the main function is to check the data for errors. When an error is detected, the data can be discarded and a retransmission can be requested. The data is considered correct at receiver side when the calculated CRC is equal to the one that was sent with the data. However, this leaves room for false negatives. A false negative arises when the data, at receiver side, is considered correct by its CRC, but the data is not equal to the original data sent by the data producer. This situation arises when the disturbance of the signal is such that both the data

and the CRC are corrupted in such a way that the disturbed CRC matches the disturbed data.

When studying CRC in the way described above, it was noted that no false negatives occurred, except in the specific cases where the disturbance frequency is an integer multiple of the bit frequency. However, in that case, the likelihood of a false negative is 50% for very strong EMI disturbances. The reason for this is that a very strong EMI disturbance pushes all sampled voltages above or below the threshold for a '1' or a '0'. This causes the output to be all ones or zeros, respectively. Unfortunately, in CRC, a data word comprising of all zeroes is considered correct, leading to a false negative. Adding a fixed offset to the CRC such that original data comprising all zeroes doesn't lead to an all-zero CRC helps to overcome the occurrence of false positives.

Hamming Codes

The Hamming Code [12][13] is a linear, Single Error Correction (SEC) code. It is one the most efficient SEC codes and was designed by R. W. Hamming in the 1950s to protect his calculations from random single bit errors. Whilst very efficient and used in many different applications, little to no attention has been paid to the effectiveness of the original Hamming Code to cope with EMI disruptions. In [12] and [13], we studied the performance of Hamming Code in the same way as described above for CRC. Specifically, we focused again on the possible occurrence of false negatives. Our research showed that for a Hamming Code there is always a certain likelihood of false negatives, but that this likelihood significantly increases when the disturbance frequency and the bit frequency are related by:

$$f_{\text{BIT}} = \frac{2f_{\text{EMI}}}{2n+1}, \text{ with n=0,1,2,...}$$

The reason for this is specific repetitiveness that can be found in valid Hamming Code words, like alternating groups of single, double,... ones or zeroes. Applying an odd parity to the Hamming Code avoids many of those repetitive patterns and decreased the likelihood of false negatives.

Triplication

Triplication [13][14] is a fault-masking technique whereby the data is sent three times over the communication channel. Once again, we investigated the effectiveness of triplication with the method described above. Four triplication variants were considered in our study. The first variant - simple triplication - is denoted as TEC, since it sends the data three times (Triplication), without inversion (Equal), bit by bit (Close together). When the data bits are interleaved within the code word, the technique is called TED, since it sends the data three times (Triplication), without inversion (Equal), with interleaving (Dispersed). Trading interleaving for inversion, the methodology is called TDC, since it sends the data three times (Triplication), with inversion (Diverse data bits), bit by bit (Close together). Finally, the last variant can use both inversion and bit interleaving. Following the same name-giving the technique becomes TDD: since it sends the data three times (Triplication), with inversion (Diverse data bits), with interleaving (Dispersed).

TEC(ABCD) = [AAA BBB CCC DDD]

TDC(ABCD) = [A$\bar{A}$A B$\bar{B}$B C$\bar{C}$C D$\bar{D}$D]

TED(ABCD) = [ABCD ABCD ABCD]

TDD(ABCD) = [ABCD $\bar{A}\bar{B}\bar{C}\bar{D}$ ABCD]

Again, we focused on the occurrence of false negatives. Our study revealed that for triplication, the overall rate of false negatives is low. However, as was the case with Hamming, specific bit rates show an increased rate of false negatives. Also, here, related to repetitiveness within valid triplication code words. Our current research focuses on improved triplication codes for which the likelihood of false negatives under strong, continuous EMI disturbances is as low as possible.

Summary and conclusions

To achieve the necessary risk-reduction within mission- or safety-critical systems against EMI disturbances, EMI-resilience has to be built into the system such that it becomes fault-tolerant against harsh EMI. This can be achieved by using, in different phases of the design process, appropriate EMI-effective T&Ms. Most of the T&Ms align with the T&Ms from IEC 61508, but modified or adopted to be (more) effective for EMI. Care has to be taken when implementing these T&Ms in a practical design as was shown with a basic study of the effectiveness of (i) hardware T&Ms like inversion, spatial, time and frequency diversity and (ii) software T&Ms like CRC coding, Hamming codes, and triplication.

References

[1] K. Armstrong, "Why EMC Immunity Testing is Inadequate for Functional Safety", Proceedings of the IEEE 2004 International Symposium on EMC, Santa Clara, CA, USA, August 9-13, pp. 145-149

[2] K. Armstrong. "Why increasing immunity test levels is not sufficient for high-reliability and critical equipment", Proceedings of the IEEE 2009 International Symposium on EMC, Austin, TX, USA, August 17-21, pp. 30 – 35.

[3] D. Pissoort and K. Armstrong. "Why is the IEEE Developing a Standard on Managing Risks Due to EM Disturbances?" Proceedings of the IEEE 2016 International Symposium on EMC, Ottawa, Canada, pp. 78 – 83.

[4] K. Armstrong, "It's EMC Jim, but not as we know it", IN Compliance, July 2015, pp. 24-35

[5] "IET Code of Practice for Electromagnetic Resilience", 2017, ISBN: 978-1-78516-324-1

[6] IEEE Standards Association, project P1848, "Techniques and Measures to Manage Risks with Regard to Electromagnetic Disturbances"

[7] J. Lannoo, A. Degraeve, D. Vanoost, J. Boydens, D. Pissoort, "Effectiveness of Inversion Diversity to Cope with EMI within a Two-Channel Redundant System", in: 2018 IEEE International Symposium on Electromagnetic Compatibility and 2018 IEEE Asia-Pacific Symposium on Electromagnetic Compatibility (EMC/APEMC), pp. 216-220)

[8] A. Degraeve and D. Pissoort, "Study of the Effectiveness of Spatially EM-Diverse Redundant Systems under Plane-Wave Illumination", in: Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC) 2016: vol. 1 (pp. 211-213)

[9] A. Degraeve and D. Pissoort, "Study of the Effectiveness of Spatially EM-Diverse Redundant Systems under Reverberation Room Conditions", in: IEEE 2016 International Symposium on Electromagnetic Compatibility (EMC) (pp. 374-378)

[10] J. Lannoo, J. Van Waes, A. Degraeve, D. Vanoost, J. Boydens, D. Pissoort, "Effectiveness of Time Diversity to Obtain EMI-Diverse Redundant Systems", in: 2018 International Symposium on Electromagnetic Compatibility (EMC Europe) (pp. 288-292)

[11] J. Van Waes, J. Lannoo, A. Degraeve, D. Vanoost, D. Pissoort, J. Boydens, "Effectiveness of Cyclic Redundancy Checks under Harsh Electromagnetic Disturbances", in: 2017 International Symposium on Electromagnetic Compatibility - EMC Europe (1-6)

[12] J. Van Waes, J. Lannoo, J. Vankeirsbilck, A. Degraeve, J. Peuteman, D. Vanoost, D. Pissoort, J. Boydens, "Effectiveness of Hamming Single Error Correction Codes under Harsh Electromagnetic Disturbances", in: IEEE International Symposium on Electromagnetic Compatibility Presented at the EMC Europe, Amsterdam, The Netherlands, Sept. 2018

[13] J. Van Waes, J. Lannoo, J. Vankeirsbilck, D. Vanoost, D. Pissoort, and J. Boydens, "Resilience of error correction codes against harsh electromagnetic disturbances: Fault mechanisms," IEEE Transactions on Electromagnetic Compatibility, 2019, submitted

[14] J. Van Waes, J. Vankeirsbilck, J. Lannoo , D. Pissoort, J. Boydens, "Effectiveness of Data Triplication in Harsh Electromagnetic Environments", in: 2018 International Symposium on Electromagnetic Compatibility - EMC Europe

Copyright of this article remains with the authors.



Connect

The Newsletter

The newsletter is published three times annually, in February, May and October and sent to paid-up members of the Safety-Critical Systems Club.

Do you have a topic you'd like to share with the systems safety community? Perhaps an interesting area of research or project work you've been involved in, some new developments you'd like to share, or perhaps you would simply like to express your views and opinions of current issues and events. If you are interested in submitting an article, then get in touch with the Newsletter Editor to discuss ideas.

The SCSC Website

Visit the Club's website scsc.uk for more details of the Safety-Critical Systems Club including past newsletters, details of how to get involved in working groups and joining information for the various forthcoming events.

Twitter

Follow the Safety-Critical Systems Club's Twitter feed for brief updates on the club and events: @SafetyClubUK

LinkedIn

You can find the club on LinkedIn. Search for the Safety-Critical Systems Club or use the following link:

www.linkedin.com/groups/3752227

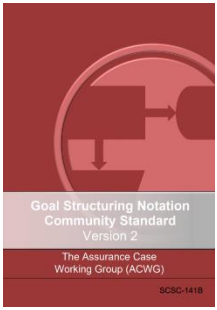
Advertising

Do you have a product, service, event or job vacancy you would like to advertise in the Newsletter? The SCSC Newsletter reaches out to over 1,000 members involved in Systems Safety and so is the perfect medium for engaging with the community. For prices and further details, please get in touch with the Newsletter Editor.

SCSC Working Groups

The Safety-Critical Systems Club is committed to supporting the activities of specialist working groups for areas of special interest to club members. The purpose of these groups is to share industry best practice, establish suitable work and research programmes, develop industry guidance documents and influence the development of standards.

Assurance Cases



The Assurance Cases Working Group (ACWG) has been established to provide guidance on all aspects of assurance cases including construction, review and maintenance. The ACWG will:

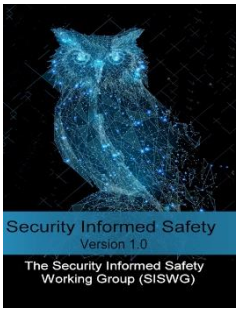
- Be broader than safety, and will address interaction and conflict between related topics
- Address aspects such as proportionality, rationale behind the guidance, focus on risk, confidence and conformance
- Consider the role of the counter-argument and evidence and the treatment of potential bias in arguments

One of the working group's initial activities is to take on board the maintenance of the Goal Structuring Notation (GSN) Community standard.

The next working group meeting is scheduled for the 18th November 2019, in London.

Lead Phil Williams phil.williams@scsc.uk

Security Informed Safety



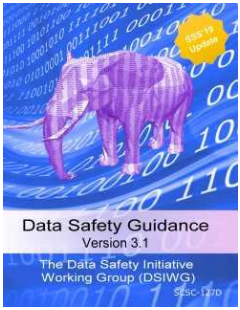
The Security Informed Safety Working Group (SISWG) aims to capture cross-domain best practice to help engineers find the 'wood through the trees' with all the different security standards, their implication and integration with safety design principles to aid the design and protection of secure safety-critical systems and systems with a safety implication.

The working group aims to produce clear and current guidance on methods to design and protect safety-related and safety-critical systems in a way that reflects prevailing and emerging best practice. The guidance will allow safety, security and other stakeholders to navigate the different security standards, understand their applicability and their integration with safety principles, and ultimately aid the design and protection of secure safety-related and safety-critical systems.

Lead Tom Turner tom.turner@scsc.uk

SCSC Working Groups

Data Safety Initiative

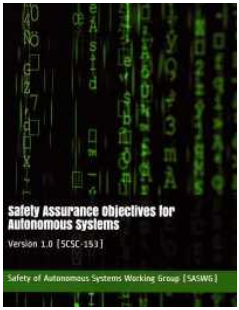


Data in safety related systems is not currently sufficiently addressed in current safety management practices and standards. It is acknowledged that data has been a contributing factor in several incidents to date. There are clear business and societal benefits, in terms of reduced harm, reduced commercial liabilities and improved business efficiencies, in investigating and addressing outstanding challenges related to safety of data.

The Data Safety Initiative Working Group (DSIWG) aims to have clear guidance on how data (as distinct from the software and hardware) should be managed in a safety related context, which will reflect emerging best practice.

Lead **Mike Parsons** mike.parsons@scsc.uk

Safety of Autonomous Systems



The specific safety challenges of autonomous systems and the technologies that enable autonomy are not adequately addressed by current safety management practices and standards. It is clear that autonomous systems can introduce many new paths to accidents, and that autonomous system technologies may not be practical to analyse adequately using accepted current practice. Whilst there are differences in detail, and standards, between domains many of the underlying challenges appear similar and it is likely that common approaches to core problems will prove possible.

The Safety of Autonomous Systems Working Group (SASWG) aims to produce clear guidance on how autonomous systems and autonomy technologies should be managed in a safety related context, in a way that reflects emerging best practice.

Lead **Rob Alexander** rob.alexander@scsc.uk

Service Assurance

Risks presented by safety-related services are rarely explicitly recognised or addressed in current safety management practices, guidelines and standards. It is likely that service (as distinct from system) failures have led to safety incidents and accidents, but this has not always been recognised. The Service Assurance Working Group (SAWG) has been set up to produce clear and practical guidance on how services should be managed in a safety related context, to reflect emerging best practice.

Lead **Mike Parsons** mike.parsons@scsc.uk

SCSC

FOR EVERYONE WORKING IN SYSTEM SAFETY

This seminar is relevant to safety engineers and safety consultants who have to perform analysis of systems. It will also be useful for safety auditors and assessors who may have to interpret or review analyses in these new methods.

Safety Analysis Techniques of the Future

scsc.uk/e654

WWW.SCSC.UK

THE SAFETY-CRITICAL SYSTEMS CLUB, Seminar:

New Safety Analysis Techniques

Thursday 11 June, 2020 - London, UK

This seminar will look at emerging, novel and recently established techniques for analysing aspects of safety systems: their overall properties, their architecture and interactions, their software, hardware and their data.

Safety systems require analysis for potential failures that can lead to hazards. Traditional techniques tend to have limited applicability in today's world of highly complex, interconnected, continually updated systems. Learning systems bring new analysis problems as the faults may be contained in the training data rather than the system itself.

Techniques such as STAMP/STPA will be covered as well as emerging methods for analysing hazards in context (Environmental Hazard Analysis). New techniques for analysing autonomous and machine learning systems will be discussed. The issues of analysing systems of systems will be covered. Tools and techniques for analysing service aspects (e.g. based on Swimlane Diagrams and Business Process Model and Notation, BPMN) and data safety will also be covered (e.g. use of data FMEA).

There will be a range of speakers covering different techniques. A wrap up session at the end of the day will discuss the most promising contenders.

The SCSC Steering Group


Tom Anderson
tom.anderson@scsc.uk


Robin Bloomfield
robin.bloomfield@scsc.uk


Stephen Bull
stephen.bull@scsc.uk


Dewi Daniels
dewi.daniels@scsc.uk


Jane Fenn
jane.fenn@scsc.uk


Paul Hampton
paul.hampton@scsc.uk


Louise Harney
louise.harney@scsc.uk


Stuart Harrison
stuart.harrison@scsc.uk


James Inge
james.inge@scsc.uk


Brian Jepson
brian.jepson@scsc.uk


Nikita Johnson
nikita.johnson@scsc.uk


Graham Jolliffe
graham.jolliffe@scsc.uk


Tim Kelly
tim.kelly@scsc.uk


Alex King
alex.king@scsc.uk


Mark Nicholson
mark.nicholson@scsc.uk


Mike Parsons
mike.parsons@scsc.uk


Felix Redmill
felix.redmill@scsc.uk


Roger Rivett
roger.rivett@scsc.uk


Phil Williams
phil.williams@scsc.uk

Calendar

October

M	T	W	T	F	S	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

November

M	T	W	T	F	S	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

December

M	T	W	T	F	S	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

January

M	T	W	T	F	S	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

February

M	T	W	T	F	S	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	

March

M	T	W	T	F	S	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

April

M	T	W	T	F	S	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

May

M	T	W	T	F	S	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

June

M	T	W	T	F	S	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					



The Principal Hotel, York – venue for SSS'20

Events Diary



9-10 Oct 2019
Conference

Lloyd's Register Foundation International Conference 2019

London, UK

https://www.lrfoundation.org.uk/en/events/lrf-conference-2019/

21-22 Oct 2019
Conference

The 14th International Conference on System Safety and Cyber Security (SSCS 2019)

London, UK

events2.theiet.org/cyber-safety

22-23 Oct 2019
Conference

7th Scandinavian Conference on System and Software Safety

Stockholm, Sweden

safety.addalot.se/2019

5 Nov 2019
Conference

High Integrity Software 2019 (HIS 2019)

Bristol, UK

www.his-2019.co.uk

12-13 Nov 2019
Workshop

First Workshop on the application of Artificial Intelligence for Systems Engineering (AI4SE 2019)

Madrid, Spain

www.kr.inf.uc3m.es/ai4se

14 Nov 2019
SCSC Seminar

Data Safety Evolution

London, UK

scsc.uk/e651

18 Nov 2019
SCSC Group Meeting

Assurance Case Working Group #10 (SCSC ACWG #10)

London, UK

scsc.uk/e648

19-20 Nov 2019
Conference

INCOSE UK Systems Engineering Conference 2019

Leeds UK

incoseonline.org.uk

5 December 2019
SCSC Seminar

Creating and Maintaining an Effective Safety Culture

London, UK

scsc.uk/e631

11-13 Feb 2020
SCSC Conference

Safety-Critical Systems Symposium (SSS'20)

York, UK

scsc.uk/e619

30 April 2020
SCSC Seminar

Safe Use of Multi-Core and Manycore Processors

London, UK

scsc.uk/e638

11 June 2020
SCSC Seminar

New Safety Analysis Techniques

London, UK

scsc.uk/e654

Safety-Critical Systems Club

SCSC

FOR EVERYONE WORKING IN SYSTEM SAFETY





28th Safety-Critical Systems Symposium

York, UK

11th - 13th February 2020

scsc.uk/e619