Pan-European Training, research and education network on Electromagnetic Risk management

(PETER)

Deliverable 5.12 – PETER Special Sessions/Workshops II @ Safety-Critical Systems Symposium (SSS'21) – Online Symposium February 9-11, 2021

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No. 812.790

Deliverable Number	**D5.12 (D34)**
Deliverable Name	**PETER Special Sessions/Workshops II**
Due Date of Deliverable	September 30, 2020
Revised Due Date Deliverable	February 28, 2021
Actual Submission Date	March 17, 2021
Deliverable Lead Partner	UTwente
Dissemination Level	Public
Work Package	WP5 Training
No of Pages (Annex not included)	4
Keywords	Special Session, Workshop, SSS2021

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

1. Prolegomena

PETER Deliverable 5.12 was initially, as stated in the PETER Grant Agreement Description of the Action Annex I Part B, foreseen to be the report of a Special Session/Workshop at EMC Europe Symposium. However, Deliverable 5.11 has been associated to a Special Session organized at EMC Europe 2020 in Rome from September 5 to 9, 2020. Deliverable 5.11 has been submitted towards the EC REA on October 15, 2020. Hence that was PETER Special Session/workshop I. By consequence, this PETER Deliverable 5.12 has been associated to a Special Session at the online Safety-Critical Systems Symposium (SSS'21) which was held online from Tuesday, February 9 until Thursday, February 11, 2021 (see also **Annex 1**: Deliverable 5.12 Deviation document).

2. Conference selection

The Safety-Critical Systems Symposium (SSS) is the main annual event of the Safety Critical Systems Club (UK). The Symposium is for all of those in the field of systems safety, including engineers, managers, consultants, students, researchers and regulators. It offers wide-ranging coverage of current safety topics, focussed on industrial experience. It covers all safety-related sectors including aerospace, defence, health, highways, marine, nuclear and rail. Keynote speakers from around the world are invited.

However, because of the COVID-19 pandemic, the organizing committee of SSS'21 had to decide to decide to move to an online-only symposium. While in past years, the physical editions of SSS covered three full days, the program now had to be limited to three afternoons of presentations, grouped into key themes together with some pre-recorded talks that attendees could watch whenever they had time for it.

As a result, the foreseen PETER Workshop had to be limited to a keynote talk by PETER's general coordinator, Prof. Davy Pissoort (KU Leuven). In addition, a full paper on the PETER project has been added to the SSS'21 Proceedings (available at https://www.amazon.co.uk/Systems-Covid-19-Proceedings-Safety-Critical-Symposium/dp/B08RRMSBTN). The paper of the keynote talk by Prof. Davy Pissoort is here attached in **Annex 2**, together with the SSS'21 brochure which can be found in **Annex 3**.

The attendance during the PETER Keynote talk on Feb 11 2021 was quite high, with on average 90 people present in the session. Through the online conference system (Whova) several discussions around the topic were started up. On Feb 24 2021, remaining questions were addressed during the follow-up SSS'21 Q&A session (ZOOM).

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

Annex 1: Deliverable 5.12 PETER Special Sessions/Workshops II Deviation document

Annex 2: Paper_SSS'21_PETER – A Pan-European Training, Research, and Education network on Electromagnetic Risk Management (Davy Pissoort, KU Leuven)

Annex 3: SSS'21 brochure

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No 812.790.
https://etn-peter.eu/

Annex 1

Deliverable 5.12 PETER Special Sessions/Workshops II Deviation document

Deviation from the PETER Grant Agreement

Description of the Action Annex 1 (part A)

DELIVERABLE 5.12 PETER Special sessions/workshops II

Safety-Critical Systems Symposium 2021: Special Session

Item:	Deliverable 5.12
Title:	~~Workshop at EMC Europe Symposium~~ **Special Session/Workshop @ SSS 2021 (Feb9-11, 2021 in Bristol)?**
Lead Beneficiary:	**~~Nedap~~ → UoY**
ERS(s) involved:	**---**
Initial Foreseen Due Date:	**September 2020**
Postponed Due date:	**February 28, 2021**

What is the **reasoning/justification** for postponing the due date for this Deliverable/Milestone/Secondment? Please explain briefly.
The MSCA PETER Project started in April 2019 and the ESRs were hired in fall 2019. The key European EMC Symposium is every year in September. So the first opportunity to organise a Special Session was September 2020. The report of this Special Session at EMC Europe 2020 has been submitted towards the EC REA via Deliverable 5.11, hence this was PETER Special session / workshop I. As a consequence and aligned between PETER consortium members, Deliverable 5.12 has been shifted till the end of February 2021 and is now associated with the PETER Special Session II at the **online Safety-Critical Systems Symposium (SSS'21) which is held from Tuesday 9 until Thursday 11 February 2021.**

What is the **mitigation plan** (Action Plan) regarding the new due date for this Deliverable/Milestone/Secondment? Also please explain briefly.
The Special Session proposal has been submitted and accepted, and the ESRs are submitting papers.

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No. 812.790.
https://etn-peter.eu/

Does this postponed due date for Deliverable/Milestone/Secondment has **any implications or consequences regarding the PETER Description of the Action as stated in the Grant Agreement Annex 1** and furthermore regarding the Project Implementation of the PETER Project? If not, please mention this specific. If so, please explain in detail which implications or consequences.
No implications since this Deviation is the logical consequence within the continuity of the PETER Deliverables regarding the foreseen Special Sessions/Workshops within the PETER Project lifetime.

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No. 812.790.
https://etn-peter.eu/

Annex 2

Paper_SSS'21_PETER – A Pan-European Training, Research, and Education network on Electromagnetic Risk Management (Davy Pissoort, KU Leuven)

PETER – A Pan-European Training, Research and Education network on Electromagnetic Risk Management

Davy Pissoort*

KU Leuven, Bruges Campus, Belgium

Abstract *Sophisticated electronic technologies are increasingly used in mission- and safety-critical systems where electromagnetic interference (EMI) can result in substantial risks to people and the environment. Currently, EMI engineering follows a rule-based approach, which is unable to cope with complex modern situations. With this rules-based approach, during the design stage, guidelines are used, which result in the application of a set of mitigation techniques, which are verified in the finished product against standards. This rule-based approach is costly, but with no guarantee of the required performance. This is particularly so for sensitive medical applications or the fully autonomous systems that are becoming ever-more common in our society. What we need is a risk-based approach, which is what PETER[1], the Pan-European Training, Research & Education Network on Electromagnetic Risk Management, will provide. PETER is training 15 young engineers in topics related to the development of high-tech systems that maintain reliability and safety over their full lifecycle, despite complex EMI, such as in hospitals or transport systems. This is achieved using best practices and state-of-the-art EM engineering, reliability engineering, functional safety, risk management and system engineering, to create the risk-based EMC approach.*

1 Introduction

Electromagnetic interference (EMI), familiar to most people as the buzzing sound from a loudspeaker when a mobile-phone call is received, is becoming much

* PETER project coordinator, professor at KU Leuven Bruges Campus. E-mail: davy.pissoort@kuleuven.be

[1] https://etn-peter.eu

Published by the Safety-Critical Systems Club.

more than just an annoyance. High-tech electronic equipment in our cars, homes, workplaces and hospitals is increasingly vulnerable to EMI. As a recent example: in May 2018, one of Mobileye's prototypes of autonomous cars went straight through a red light about a quarter of mile from the company's garage after an otherwise uneventful ride. And, of course, this happened at well-attended press release. Mobileye's Chief Executive Officer Amnon Shashua said wireless transmitters on cameras used by the television crew created electromagnetic interference, which disrupted signals from a transponder on the traffic light[2].

What all this means is that as technology advances and we are able to produce machines like autonomous vehicles, which are likely safer than those driven by humans, the problem of EMI-related risks does not simply go away. Instead, we need to shift our focus away from the relatively visible risks associated with conventional devices, to understanding how the enormously complex systems that we are constructing around us are also susceptible to risk, but a different kind of risk that is associated with invisible EMI. So, as advances in medicine lead to greater survival rates after surgery, for example, and to fewer post-operational problems, the number of reported incidents in hospitals relating to EMI is also steadily increasingly, as a search in the US MAUDE database reveals (Fig. 1). Paradoxically, at the same time as we improve the quality of lives, reducing many familiar risks and allowing people to enjoy a lot of things that were not available to them less than a generation ago, we expose ourselves to other dangers like EMI that require a very different approach to managing risk in complex scenarios.

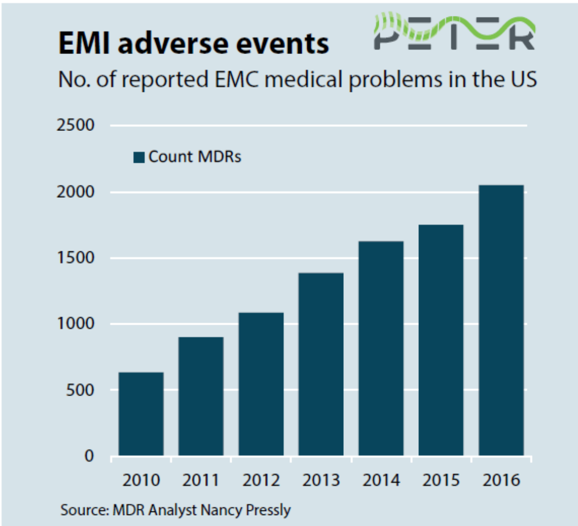

Fig. 1. Increase in the number of electromagnetic interference medical events in the US

[2] https://www.bloomberg.com/news/articles/2018-05-21/why-intel-s-mobileye-blew-a-red-light-while-showing-off-its-ride (accessed on Nov 30 2020)

To get an idea of how the problem of EMI could develop as electronic equipment becomes more complex and we become increasingly reliant on its dependability, let's expand on a couple of very plausible scenarios. Imagine an explosion at an aging chemical plant. Firefighters arrive quickly, bringing the usual hoses and ladders, but also the latest high-tech camera drone to assess the extent of the damage and identify the access paths through the site. While leading the firefighters through the smouldering remains of the plant, the drone flies too close to the plant's old wireless-communication system and is exposed to a higher field strength than it is designed and tested for. The remote operator of the drone sees the system crash, and with it the drone. Fortunately, no one is hurt that day, but the firefighters have a lucky escape. In the second example, a big-city hospital is involved in a remote surgical operation. A woman is having a craniectomy, with the knife being wielded by a robot, controlled by a surgeon sitting in a room more than 2000 km away. This is one of the most dangerous and difficult operations, performed by only a few of world's leading specialists. During the final stages an electrosurgical procedure is required, which involves a radio-frequency electric surgery knife. Instantly, the images on the monitors become distorted, the LED status lights flicker ominously, and a human life is in danger.

1.1 The flaws in the current "rule-based" approach

Currently, the problem of EMI is adressed using a "rule-based" approach. What this means is that during the design phase for a piece of electronic equipment a number of guidelines/standards (e.g. the IEC 61000-x series) are used resulting in the default application of a set of mitigation techniques (filtering, shielding, cable routing, etc.). But as the examples above illustrate, such an approach has some serious flaws when it comes to modern high-tech systems and high-safety criticality applications like medical systems and remotely driven vehicles. This is because tackling the problem by applying rules leads to too many failure scenarios being overlooked and giving us false confidence when it comes to how reliable and safe a new system actually is. Therefore, in order to make sure that people's safety is not compromised in this way, the PETER consortium is developing a novel and much more robust "risk-based" approach to EMI management.

The weakness of the rule-based approach is that it has several major shortcomings. Firstly, we have no certainties when it comes to knowing whether these mitigation strategies, or rules, are really sufficient. Even if we could be sure of this, most of us know from experience that standards always lag behind technological developments and are based on economic and technical compromises. Perhaps the biggest worry is that immunity testing in electromagnetic compatibility standards only covers one EMI disturbance at a time, meaning that simultaneous EMI effects are not addressed. While such simultaneous EMI effects would easily occur in practice, e.g. someone making a phone call while at the same time touching a display. The first generating electromagnetic fields in the air and the latter possibly leading to an electrostatic discharge. Added to this we have the problem that the testing of large installations is limited to just the subsystems being evaluated when they are brand new. But of course, EMI is a “whole system” property with many of the effects resulting from environmental factors like ageing, vibration, and temperature, as well as manufacturing variability or the impact of maintenance, repairs and upgrades.

1.2 PETER’s solution: a risk-based approach

What is needed is a truly interdisciplinary – but also revolutionary – approach to this very serious problem. A safer environment based on assessing risk requires bringing together expertise from four operating key areas – electromagnetic compatibility, reliability engineering, functional safety and risk management – and the implementation of a risk-based approach. The PETER project – which started on April 1st 2019 and will run for four years - will consider the complete system over its whole lifecycle, i.e., from the earliest concept to the final decommissioning. The risk-based approach, which will eventually replace the out-dated rule-based approach in high tech systems, involves 3 steps: hazard-and-risk analysis, risk reduction, verification and validation.

PETER’s main goal is to train 15 early-stage researchers (ESRs) in topics related to the development of high-technology systems that maintain reliability and safety over their full life-cycle, despite these systems being subjected to severe and complex EMI threats.

2 PETER’s Consortium

The PETER project involves an European-wide consortium of 13 Beneficiaries and six Partner Organisations from five EU countries (see Figure 2). Of the 13 Beneficiaries, six are from industry and two are industry-oriented research centres, which will give the 15 ESRs tremendous opportunities to obtain industry-relevant training.

The PETER Beneficiaries are six high-technology companies, including Barco and Melexis (BE), Nedap and RHM (NL), MIRA (UK), and Valeo (FR), two non-university research institutes, WIS and FHG (GE), and 5 universities, KU Leuven (BE), LUH (GE), UTwente (NL), UoY (UK), and ESEO (FR). The consortium is completed by six Partner Organisations that include four companies, a hospital and a university.

Fig. 2. Map showing the locations of the PETER Beneficiaries and Partner Organisations, together with the Network-Wide Events and Site Visits

3 PETER's Work Package Structure

PETER has four scientific and technical (S&T) objectives based around four S/T Work Packages (WPs), see Figure 3:

- To develop dedicated hazard-and-risk analysis techniques that identify all EMI-related risks and hazards for a system under development in its actual operating electromagnetic environment, including the possibility of malicious EMI (WP1).
- To develop effective EMI risk-reduction techniques in hardware and software, and to reduce the risks to the level where they are no longer unacceptable with respect to reliability or safety (WP2).
- To improve EMI verification-and-validation methods that represent a much broader area of the lifecycle of the system as well as of the system's actual electromagnetic environment (WP3).

- To apply a practical, industry-driven EMI risk-management methodology during four case studies, from different industrial sectors (maritime, medical, automotive, critical infrastructures) and at different design levels (integrated circuits, subsystems, systems and networks of systems) (WP4).

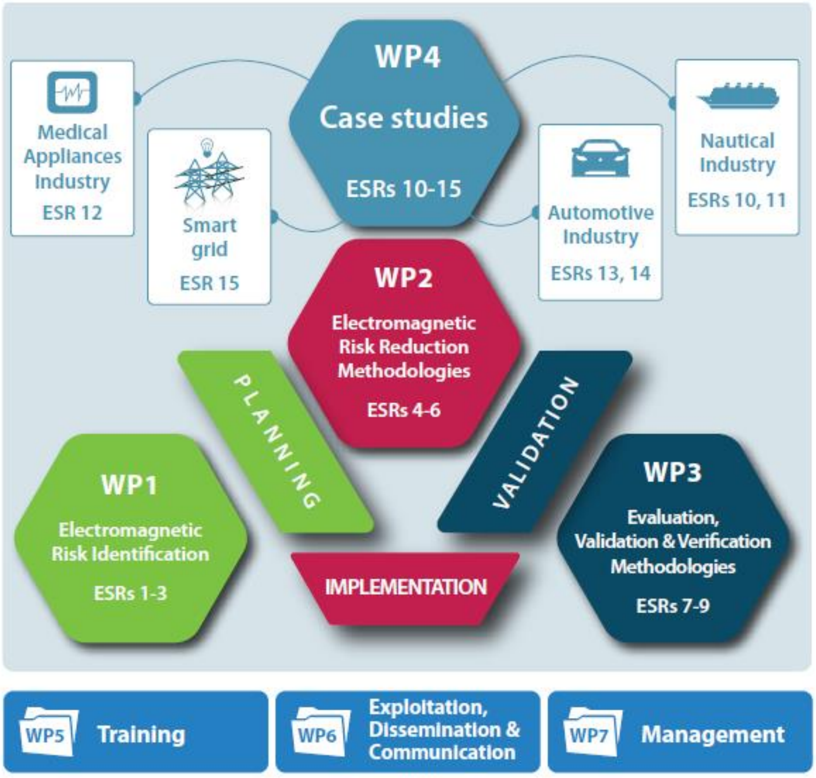

Fig. 3. PETER Work Package Overview

3.1 WP1: Electromagnetic Risk Identification

WP1 involves three ESRs and focuses on the left part of the V-model (Figure 3) as the first step in a complete risk-based approach, i.e. the identification of all the potential EMI-related risks and their criticality. ESR1 and ESR2 take up the challenge of *developing a generic electromagnetic risk-analysis methodology applicable to large and complex systems.* This procedure extends the current interference descriptions of separate subsystems to a generic risk description of the whole interconnected system, e.g., from a smart machine to a critical infrastructure. It will take into account possible non-technical aspects (accessibility, regulations, etc.). ESR1 and ESR2 will be working closely on complementary projects, with ESR1 having the task of laying the theoretical fundamentals of the risk-analysis methodology, while ESR2 provides the experimental analysis and verification.

Starting from the perspective of automotive applications, ESR3 will focus on a *risk-based electromagnetic engineering approach aligned with the ISO 26262 Functional Safety approach*. The great challenge here is that this approach should cover safety, cybersecurity and functional performance. As such, it will be aligned with ISO 26262 functional safety concepts and the SAE Cybersecurity Guidebook, as well as integrating computational electromagnetics results within classic hazard-and-risk analysis methods (fault-tree analysis, failure-mode and effect analysis, etc.).

3.2 WP2: Electromagnetic Risk-Reduction Methodologies

WP2 tackles the actual design of the mission- or safety-critical systems with three ESRs focusing on techniques and measures that effectively reduce the risks (identified with the methods of WP1) to the level that they no longer represent unacceptable reliability or safety risks.

The first of these ESRs, ESR4, is going to look at the overall *risk-based EMI-aware design of complex systems*. Starting from the risk identification (ESRs 1–3) together with a decomposition of the electromagnetic environment into tangible levels, an EMC risk-management plan (EMI-RMP) will be established. Following system-engineering principles, this EMI-RMP will drive the design, operational use and maintenance of the system. In collaboration with the other ESRs, an EMI-RMP will be made for future vehicle-to-X communication systems, complex maritime systems, medical display systems inside a hospital, and a typical smart grid.

During the design, the EMI-RMP will also identify which risk-reduction techniques should be chosen and implemented. Originally, the hardening techniques (both hardware and software) used within reliability engineering and functional safety were not developed for EMI. Hence, they will need modification and optimization to be effective for EMI, thereby also fitting EMI into the safety assessment workflow a part of the Preliminary System Safety Assessment (PSSA) process. To overcome this challenge, ESRs 5 and 6 will be working on cost-effective *IEC 61508 Techniques & Measures for EMI Risk Reduction* and this for *hardware-based and software-based techniques and measures*, respectively. Thanks to the developed techniques & measures, a significant step-forward will be achieved in the design of high-tech medical display systems, automotive communication systems, and the smart grid.

3.3 WP3: Evaluation, Validation and Verification Methodologies

WP3 targets novel methodologies that allow us to evaluate, validate and verify that the applied risk-reduction techniques (WP2) have been implemented correctly and that they effectively address the identified risks (WP1) over the full lifecycle. It is crucial that the analysis takes into account the full lifecycle (environmental stresses, ageing, replacement of components during maintenance etc.). Once again, two ESRs, ESRs 7 and 8, will be working together on closely related, but complementary, research topics. While they both study simulation models and testing methods for the *evaluation of electromagnetic hazards due to environmental stresses, obsolescence and/or ageing*, their specific focus is different. ESR7 focuses on the level of the electronic components (integrated circuits), while ESR8 focuses on the system level. ESR7 will apply his/her models and methods to an automotive integrated circuit in collaboration with ESR14 (WP4). ESR8 will assist ESR5 (WP2) in the validation process for the optimized IEC 616508 techniques and measures under extreme stress.

Given the complexity of current electromagnetic environments, the way electromagnetic disturbances interact with a system will become extremely sensitive to small variations. Thus, just as for the risk assessment, statistical techniques will need to be integrated into the classic EMC testing. Therefore, ESR9 will develop a methodology for the *statistical verification and validation of immunity and enclosure shielding effectiveness*. Evidently, this statistical verification and validation should have a lot in common with the statistical risk analysis developed by ESRs 1 and 2. Finally, together with ESR7, the statistical verification and validation will be applied to an automotive integrated circuit (ESR14, WP4).

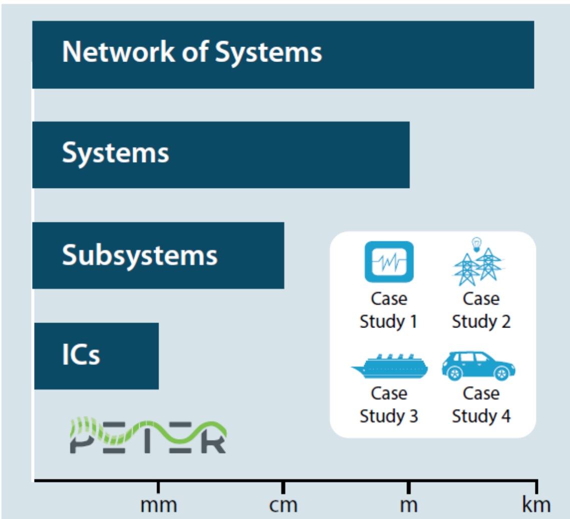

Fig. 4. PETER's four case studies at 4 different design levels

3.4 WP4: Application Case Studies

The PETER WPs conclude with WP4, which pilots the full risk-based EMC approach, combining the previous three research tracks, thereby enabling the shift from rule-based to risk-based EMC approaches. In total, six ESRs are working on case studies for four different industrial sectors: maritime, healthcare, automotive and an energy network infrastructure in the form of a smart grid. Moreover, the case studies cover four different design levels (Fig. 4): integrated circuits (mm scale), subsystem (cm scale), system (m scale) and network of systems (km scale). These case studies will not only use the results of the ESRs from WPs 1–3, but will also provide essential practical feedback for them.

ESR 10 and 11 both focus on maritime applications. ESR10 aims at *cost-effective, up-to-date, maritime* EMC standards *that move away from the rule-based approach to a risk-based approach*. ESR11 will *model and reason about electromagnetic interactions in autonomous and complex vessels*. ESR12 applies the risk-based EMC approach to the medical sector through the *design of* EMI-resilient *medical display systems for surgical-, diagnostic imaging- and modality applications*. Both EMI and functional safety will become increasingly important within automotive applications as we shift towards self-driving, interconnected vehicles. Hence, ESRs 13 and 14 address two significant challenges related to vehicles of the future. ESR13 applies the *EMI risk management to the next generation of vehicle communication devices*, while ESR14 designs *an automotive integrated circuit through a risk-based and* EMI-aware approach. Finally, ESR15 has the task of *managing in the* EMI risks *on the scale of the smart grid as a network of systems*.

4 Conclusions

The goal of PETER is to achieve a risk-based approach to addressing EMI. In so doing, it will also train the researchers in this area to provice continued activities after the end of the programme. PETER proposes an interactive approach where EMI is taken into account during all the phases of a risk-management process and where this is directly applied to industry-driven application case studies. PETER will provide the first-ever high-quality interdisciplinary training in the field of risk-based EMC to 15 talented ESRs through research, taught courses and Network-Wide Events, covering scientific aspects as well as personal skills and career development.

During the PETER proposal-building phase we made sure that industry would play a major role in the project and that many aspects of the project would be industry led. Only by integrating the real-world experience of companies that succeed through their own excellence and ability to innovate and adapt can we be in a position to train the ESRs to see innovation as fundamental to their research. Every one of the 15 ESRs' PhD projects was assessed and then approved by the industry Participants – Beneficiaries and Partner Organisations – in terms of its innovation potential in the European context. What we are aiming for in the PETER project is to have ESRs who see research as an opportunity to innovate, to look at problems from a new perspective, and to see the potential for marketing their ideas and knowledge.

Finally, through the participation of the ESRs and supervisors in the IEEE P1848 and IEC 61000-1-2 standardization committees, PETER aims at a strong contribution to European standardisation.

Acknowledgments The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie Grant Agreement No 812.790 (MSCA-ETN PETER). This publication reflects only the authors' view, exempting the European Union from any liability. Project website: http://etn-peter.eu/.

Annex 3

SSS’21 brochure

Safety-Critical Systems Club

SSS'21 Programme

29th Safety-Critical Systems Symposium

Virtual Conference

9th - 11th February 2021

SCSC

FOR EVERYONE WORKING IN SYSTEM SAFETY

The Safety-Critical Systems Club invites delegates to its Twenty-Ninth Annual Symposium

Our world has changed dramatically over the last year with the Covid-19 pandemic, and life will not resume to normal for some time. This is our first online-only symposium changing the way we have done things historically but also bringing new opportunities.

The management of the pandemic has used systems like never before: everything from models predicting the spread of the disease to thermal scanners at airports and contact tracing apps on phones. New systems and services have been developed or re-purposed to assist in record time, but assurance of these solutions is missing in many cases. There is no doubt that many of these solutions are now safety-related, and lives have been affected by failures, e.g. in Track & Trace.

However, our more usual fare of engineering-led solutions have continued development through the last year. The Boeing 737 MAX took far longer than expected to resume to service reflecting the many fundamental issues that were found with the aircraft and its systems and software.

Operators, users (and the general public) now cannot understand the complexity inside systems ensuring safety and cannot be relied upon to take over if the systems fail suddenly. We need to recognize this and design systems to be both fail-safe and to be able to explain their failures wherever possible.

The SCSC Working Groups have been developed and expanded to cover areas where there are areas for improvement: in Multicore and Manycore processor based systems, in Safety Culture, in underlying Risk Ontologies and also in systems used for Covid-19 management. The existing groups for Assurance Cases, Autonomous Systems, Data Safety, Security Informed Safety and Service Assurance have all continued throughout the year.

This symposium will tackle many of these new challenges and present work towards solutions.

The Safety-Critical Systems Club has operated in support of the safety community since 1991. This is the programme for the **29th Club Symposium in February 2021**.

SSS'21 extends across three afternoons of presentations, grouped into key themes. The keynote speakers are: Robin Bloomfield, John Holmes, Peter Ladkin, Davy Pissoort, Harold Thimbleby and Simon Whiteley. Emma Taylor and Patrick Hudson will be giving special talks. We are particularly pleased to welcome back Tim Kelly, our past director of the club, who will give a special introductory talk.

Key features are:

- Website and Whova areas: scsc.uk/e683
- Six keynote presentations;
- Primary themes of: Covid-19, Embedded Systems, Future Assurance, Internet of Things (IoT), Software, Security Informed Safety and Human Factors and Safety Culture;
- Updates from the SCSC Working Groups;
- Virtual exhibition and poster area;
- Proceedings book with papers for presentations and posters

THE SAFETY-CRITICAL SYSTEMS CLUB

Safety-Critical Systems Symposium (SSS'21)

The programme encompasses three afternoons and one evening of presentations including six keynote talks, submitted papers, an online poster room, interactive sessions, updates from the SCSC Working Groups, and an online vendor exhibition.

Tim Kelly will be opening the symposium with a special introductory talk, 'Thought for the Symposium'. Six eminent speakers have kindly agreed to give keynote talks. There are two additional 'after-dinner' talks on the Wednesday evening.

Symposium Website and Whova areas: scsc.uk/e683

Introductory Speaker

Tim Kelly worked for over 25 years in the domain of high-integrity and safety-critical systems engineering. In 2019 he took a 'leap of faith' and gave up being a full-time Professor in High Integrity Systems at the University of York to become a vicar in the Church of England, and has recently moved to Beverley Minster. To some this would be seen as a risky move! Risk unifies us all. We all have to manage risk in our daily lives. In his introductory talk Tim will talk about how risk forms a thread that connects his past and current roles. He'll describe how his experiences in the safety domain have translated to his new role and career, including entertaining ideas such as whether ALARP (As Low As Reasonably Practicable) has a role to play in the life of the church, whether autonomous systems can follow Jesus' command to love one another, and whether sermons could benefit from applying the Goal Structuring Notation (GSN).

Keynote Speakers

The Keynote speakers are: Robin Bloomfield, John Holmes, Peter Ladkin, Davy Pissoort, Harold Thimbleby and Simon Whiteley.

Robin E Bloomfield FREng is a founder of the specialist safety and security consultancy Adelard LLP. He is also a full Professor at City University London. His work in safety and security in the past 30 years has combined policy formulation, technical consulting and underpinning research. He was elected a Fellow of the Royal Academy of Engineering in 2014 in recognition of his international leadership in the engineering of safety-critical systems containing software. He is a major contributor to the development of the assurance and safety case approach and the use of claims, arguments and evidence (CAE) and the extension of this work to security and critical infrastructures. His current focus is on trustworthiness of systems using AI/ML as well as on the automation of certification

John Holmes is a Chartered Engineer and Fellow of the Royal Aeronautical Society. He has worked all his career in aviation both as a provider and a regulator of Air Traffic Services, starting on surveillance systems, and has worked on a wide range of projects including the relocation of Terminal Control from West Drayton, and the new Prestwick Centre. John is currently employed by NATS as the Principal Specialist, Safety Management System and Commercial Space.

Peter Ladkin is Professor of Computer Networks and Distributed Systems in the Faculty of Technology at the University of Bielefeld; Principal Investigator in the university's Cognitive Interaction Technology Center of Excellence CITEC; founder and a director of the tech-transfer company Causalis Limited.

Davy Pissoort is Professor at KU Leuven, Bruges Campus in Belgium, where he is one of principle investigators in the Mechatronics Group (M-Group). His research interests include Electromagnetic Interference, Electromagnetic Risk Management as well as overall safety assurance of interconnected mechatronic systems. Davy Pissoort is a Senior Member of the IEEE EMC Society, IEEE EMC Society Board Member and member of the International Steering Committee of EMC Europe. He is currently coordinating two Marie Skłodowska-Curie Actions Training Innovative Training Networks under the Horizon 2020 framework. The first one on the topic of Safer Autonomous Systems (www.etn-sas.eu) and the second one on the topic on a Risk-Based Approach to Manage (Safety-related) Risks due to Electromagnetic Disturbances (www.etn-peter.eu). In his keynote talk, Davy Pissoort will describe the increasing safety-related risks that electromagnetic interference brings along for autonomous systems and give an insight in the latest risk-based techniques to manage these risks.

Harold Thimbleby is See Change Fellow in Digital Health, based at Swansea University in Wales. Professor Harold Thimbleby is Expert Advisor on IT to the Royal College of Physicians, a member of the World Health Organization's Patient Safety Network, Patient Safety Council Member of the Royal Society of Medicine, and an advisor to the Clinical Human Factors Group and to the UK Medicines & Healthcare products Regulatory Agency (MHRA). Harold has been invited to talk in over 30 countries.

Simon Whiteley is a System Safety Engineering Consultant at Whiteley Aerospace. He has a BEng in Aerospace Engineering and an MSc in Safety Critical Systems Engineering. Simon trains, coaches and consults with individuals and organisations globally (including both businesses and world-renowned academic institutions), across diverse industry sectors and supports them in achieving fantastic results using STAMP, STPA & CAST. Simon has worked across many industry sectors including Civil & Defence Aerospace, Air Traffic Control (ATC), Weapon Systems, Maritime, Defence Nuclear, Automotive / Autonomous vehicles / Systems, Healthcare & Government IT, Rail, Pharmaceuticals & Energy (Oil & Gas).

Special Speakers

Emma Taylor will give a special talk on communications and persuasion and how, as safety professionals, we need to focus on appropriate communications with our stakeholders.

Patrick Hudson will give an interesting and entertaining talk in the “after-dinner” slot. His talk is entitled *“Safety Culture Stories: News from the Front”*.

John McDermid will bring us up to date on the Royal Academy of Engineering *“Safer Complex Systems”* initiative.

Emma Ariane Taylor is a Chartered Engineer with over 25 years’ experience across multiple sectors: rail, oil and gas/energy and space and highly regulated environments. Emma has a strong track record in stakeholder management across NGO, government and commercial sectors and has technical, commercial and operational leadership. She was Chair of the Safety and Reliability Society (SaRS) in 2019 also a UK Engineering Council Professional Affiliate, a Charity Trustee (UK Charities Commission) and a Company Director. She was recognised in the 2019 Financial Times and Inclusive Boards 100 Influential Women in UK Engineering and by the 2018 Daily Telegraph Top 50 Women in Engineering.

Patrick Hudson is a psychologist with wide experience of safety and management in a variety of high-hazard industries. He has worked with the Oil and Gas sector, both upstream and downstream, commercial and military aviation, shipping, mining and hospital medicine. He was one of the developers of the Tripod model for Shell, together with Jim Reason and Willem Wagenaar, better known as the Swiss Cheese model. He was part of Shell's team developing the theory of SMS in response to Piper Alpha and is now involved in teaching and developing SMS concepts in Civil Aviation, primarily in Asia and Australasia. He developed the HSE Culture ladder, together with Dianne Parker and is now working on improving concepts of risk analysis in hospital medicine, transferring knowledge and experience between industries. He is emeritus professor at Delft University of Technology in The Human Factor in Safety at the Department of Safety Science.

John McDermid Professor John McDermid OBE FREng is Director of Assuring Autonomy International Programme at the University of York. He is also a Non-Executive Director at the UK Health and Safety Executive.

Vendor Exhibition

The exhibition will be online in a special dedicated virtual space. **For exhibition opportunities, please contact Alex King, alex.king@scsc.uk**

The Symposium Team

Four key people make this online symposium happen. They are:

Mike Parsons

Alex King

Mark Nicholson

Brian Jepson

Day One - Tuesday 9th February 2021: scsc.uk/e683

Introduction

14:00 – 14:10	Mike Parsons, SCSC	Welcome and Introduction
14:10 – 14:30	Tim Kelly, Church of England	Thought for the Symposium

Systems View of Covid-19
Chair: Mike Parsons

14:30 – 15:05	**Keynote**: Harold Thimbleby, See Change Digital Health Fellow	**The pivotal pandemic: Why we urgently need to fix IT**
15:05 – 15:40	**Keynote:** Simon Whiteley, Whiteley Aerospace	**What can be learned from the UK response to the Coronavirus using STAMP and how this learning could shape future responses & policies**
15:40 – 15:50	Comfort Break	
15:50 – 16:25	**Keynote**: Peter Ladkin, Causalis Ingenieurgesellschaft mbH	**Confounding Covid**
Pre-recorded	Nicholas Hales, Retired Senior Engineer for Critical Avionics	**Data Safety in Virus Outbreaks: Lessons Learnt and Recommendations**
Paper-only	Peter Bernard Ladkin, Causalis Ingenieurgesellschaft mbH	**Chances, Confidence and Risks Analysis: The Chance of Covid-19 Infection in the Day Care of Very Young Children**

Internet of Things (IoT)

Pre-recorded	Kai Barrington, Ian Burgoyne, James Edwards, Adrian Jones, Wendy Owen, COSTAIN	**Meerkat – IoT-Based Solar-Powered SIL2 Footpath Level Crossing Warning System**
Pre-recorded	Michael Green, Ecomergy	**Safety-critical wireless communication links**

Software
Chair: Dave Banham

16:25-16:55	Chris Hobbs and Waqar Ahmed, BlackBerry QNX	**Using Bayesian Modelling to Predict Software Incidents**

SCSC Updates

Pre-recorded	Zoe Garstang, BAE Systems	**SCSC Safety Futures Initiative**
Pre-recorded	SCSC Working Group Leaders	**Assurance Cases, Autonomous Systems, Covid-19, Data Safety, Multicore, Ontology, Safety Culture Security Informed Safety, Service Assurance**

https://www.surveymonkey.co.uk/r/9ZDJTXQ

Day Two - Wednesday 10th February 2021: scsc.uk/e683

Future Assurance
Chair: Jane Fenn

14:00 – 14:35	**Keynote:** Robin Bloomfield, Adelard / City University and John Rushby, SRI International	**Assurance 2.0: A Manifesto**
14:35 – 15:05	Yvonne Oakshott, Leonardo; Paul Chinneck, RINA	**Six Honest Serving Men for Today (Dialectic Argumentation for Assurance Cases)**
15:05 – 15:35	Ibrahim Habli, Rob Alexander and Richard Hawkins, University of York	**Safety Cases: An Impending Crisis?**
15:35 – 15:45	Comfort Break	
15:45 – 16:15	Kevin King, BAE Systems and Mark Nicholson, University of York	**Digital Twins for Safety-Critical Systems: Principles to support their role in safety assurance**
Pre-recorded	J Calford, C Allsopp, R Gambon, Frazer-Nash Consultancy; K Eder, University of Bristol; J Smith, University of the West of England, R Maguire, Dstl	**Assuring the Integration of Autonomy: A Fault Taxonomy**

Human Factors and Safety Culture

Pre-recorded	Michael Wright, Greenstreet Berman Ltd and Stuart King, Energy Institute	**Safe staffing levels: latest Energy Institute guidance**
Pre-recorded	David Pennie, Greenstreet Berman Ltd	**Human reliability assessment procedure for non-Human Factors practitioners**

Evening Session (After-Dinner)
Chair: Tom Anderson

19:00 – 19:30	Emma Ariane Taylor, SaRS	**Influencing for Safety and Risk: A Novel Toolkit**
19:30 – 20:00	Patrick Hudson Hudson Global Consulting & Delft University of Technology; Timothy Hudson Tim Hudson Consulting	**Safety Culture Stories: News from the Front**
Pre-recorded	Michael Ellims, Sybernetic Ltd.	**A Longitudinal Study in Medical Error: The Limits of Lists**
Pre-recorded	Simon Burton[1,2], John McDermid[1], Philip Garnett[1], and Rob Weaver[3] [1]University of York; [2]Fraunhofer Institute for Cognitive Systems; [3]Independent Consultant	**An Initial Framework Assessing the Safety of Complex Systems**

https://www.surveymonkey.co.uk/r/959HBP5

Day Three - Thursday 11th February 2021: scsc.uk/e683

EMI/EMC **Chair: Mark Nicholson**		
14:00 – 14:35	**Keynote:** Davy Pissoort, KU Leuven	**PETER – A Pan-European Training, Research and Education network on Electromagnetic Risk Management**
Security Informed Safety **Chair: Stephen Bull**		
14:35 – 15:05	Arlen Baker, Paul J. Parkinson Wind River	**IPnet Vulnerabilities: A case study**
Pre-recorded	Lee Ramsay, Mick Warren Frazer-Nash Consultancy Ltd	**Challenges of Cyber-Resilience in Aviation: An Implementation**
New Techniques **Chair: Roger Rivett**		
15:05 – 15:35	Matt Osborne, Mark Nicholson, Richard Hawkins, University of York	**An "As Desired" Model of the Software Safety Assurance Lifecycle**
15:35 – 15:45	Comfort Break	
15:45 – 16:15	Mark Sujan[1], John Watt[2], Riccardo Patriarca[3], Francesco Costantino[3], Maria Luisa Villani[4] and Antonio de Nicola[4] [1]Human Factors Everywhere; [2]Middlesex University; [3]Sapienza University of Rome; [4]ENEA	**Developing Leading Safety Indicators using the Functional Resonance Analysis Method**
16:15 – 17:20	**Keynote**: John Holmes	**The Future of Satellite Launch From the UK**
17:20 – 17:25	Mike Parsons	Closing Remarks
Pre-recorded	Masao Ito, NIL Inc	**TM Card: A way to provide a useful index for standards and guidelines for Autonomous Vehicles**
Paper-only	Peter Bernard Ladkin, Causalis Ingenieurgesellschaft mbH	**A Simple Calculus of Confidence**
Pre-recorded	Anil Ranjitbhai Patel, Nikita Bhardwaj Haupt, Peter Liggesmeyer, SEDA, TU Kaiserslautern	**Prediction of Dynamic Adaptation Technique for Autonomous Vehicles using Decision Trees**
Embedded Systems		
Pre-recorded	Iain Bate, University of York, Louise Harney, Leonardo MW Ltd	**Open Challenges and Gaps in the Guidance for the Use of Multi-Cores and MPSoCs in Safety-Critical Systems**
Pre-recorded	Dave Banham, Michael Brown, BlackBerry QNX	**The impact of Über-Authorities on WCET**

https://www.surveymonkey.co.uk/r/95RBYN5

Cost

The event is free to members of the club.
Please see scsc.uk/membership.
Contact Alex King (alex.king@scsc.uk) for further details and concessions.

Streaming and Access Details

Website and Whova: scsc.uk/e683
Further details will be emailed to registered delegates.

Registration

All enquiries to: Alex King, Department of Computer Science, University of York, Deramore Lane, York, YO10 5GH. Phone: 01904 325402, Fax: 01904 325599, Email: alex.king@scsc.uk

Department of Computer Science, University of York
Phone: 01904 325402 Fax: 01904 325599 Email: alex.king@scsc.uk

---

The full proceedings of the symposium will be available from the SCSC website as a PDF. They are currently available in hardcopy form as a book from Amazon