Amsterdam University of Applied Sciences

# International Cross-Industry Safety Conference (ICSC) and European STAMP Workshop & Conference (ESWC) 2018

# Editorial of Proceedings

**Nektarios Karanikas**[1], **Maria Mikela Chatzimichailidou**[2] **and Martin Rejzek**[3]
[1]Aviation Academy, Amsterdam University of Applied Sciences, the Netherlands
[2]WSP & Imperial College London, United Kingdom
[3]Zurich University of Applied Sciences, Switzerland

The Amsterdam University of Applied Sciences organised in Amsterdam (31 October - 2 November 2018) the 3rd edition of the International Cross-industry Safety Conference (ICSC) and the 6th edition of the European STAMP Workshop & Conference (ESWC) dedicated to both practical and theoretical aspects of safety. The conferences functioned as platforms to share and transfer knowledge about safety within and across industry and academia.

Geleyn Meijer (Rector of the Amsterdam University of Applied Sciences, NL) opened the event and Stephan Berndsen (Investigation Manager at the Dutch Safety Board, NL), George Boustras (Professor in Risk Assessment at European University Cyprus and Editor-in-Chief of Safety Science, CY), Pier Eringa (Chairman of the Board of Directors, ProRail, NL) and John Thomas (Massachusetts Institute of Technology, US) addressed the conferences as keynote speakers. Besides the keynote speakers, 39 delegates from various industry, academia and (inter)governmental organisations delivered their presentations and discussed with the attendants a wide range of practical applications and research results.

We would like to thank:

- ICAO for their support to the event
- Aegean Airlines (GR) and Kindunos Consultancy (NL) for their kind sponsorship
- The library of the Amsterdam University of Applied Sciences for sponsoring the ICSC and ESWC 2018 proceedings

We would also like to thank the organising committee members Nick Leegstra and Rianne Boute under the leadership of Sanne van Dorp. Finally, we express our deep appreciation to the program committees' members for their efforts to review the abstracts and full papers (in alphabetical order of the last name):

- International Cross-industry Safety Conference
  - James Catmur, JC&A Ltd., UK
  - Steve Denniss, WSP, UK
  - Kubra Kaya, University of Cambridge, UK
  - Genovefa Kefalidou, University of Leicester, UK
  - Angela Ku, Jacobs, UK
  - Alberto Martinetti, University of Twente, NL
  - Catherine Menon, University of Hertfordshire, UK
  - Jan Przydatek, Lloyds Register Foundation, UK
  - Alfred Roelen, Netherlands Aerospace Centre, NL
  - Emma Taylor, RSSB, UK

- European STAMP Workshop & Conference
  - Asim Abdulkhaleq, Robert Bosch GmbH, GE
  - Svana Helen Björnsdottir, Stiki Information Security, IS
  - Robert J. de Boer, Amsterdam University of Applied Sciences, NL
  - Ioannis Dokas, Democritus University of Thrace, GR
  - Þórður Víkingur Friðgeirsson, Reykjavik University, IS
  - Sven Stefan Krauss, Zurich University of Applied Sciences, CH
  - Anastasios Plioutsias, National Technical University of Athens, GR
  - John Thomas, Massachusetts Institute of Technology, US
  - Stefan Wagner, University of Stuttgart, GE
  - Simon Whiteley, Whiteley Aerospace Safety Engineering & Management Limited, UK

The conference would not have been possible without the commitment of all these individuals.

In this editorial, we append the abstracts of the contributions that were not submitted as full papers. We hope that the full papers as well the themes covered by the abstracts will trigger the readers to reflect on their practice and safety initiatives and contact the contributors for any inquiries and possible collaborations.

Judging from the variety of the presentations as well as their content and quality, we are convinced that the 3rd edition of the ICSC and the 6th edition of the ESWC were successful and served their intended scope. We look forward to welcoming you to the next editions of the ICSC and ESWC!

Dr Nektarios Karanikas, Chair of ICSC and ESWC 2018

Dr Maria Mikela Chatzimichailidou, Co-chair of ICSC 2018

Martin Rejzek, Co-chair of ESWC 2018

*3rd International Cross-industry Safety Conference*
*31 October-2 November 2018, Amsterdam*

# Social Complexities: The Missing Link in Critical Incident Reporting Systems

**Jaco van der Westhuizen[1,*] and Karel Stanz[2]**
[1] Air Traffic & Navigation Services, South Africa
[2] University of Pretoria, South Africa

## ABSTRACT

The safe operation of complex socio-technical systems depends on the information that flows in each system. Prior research on critical incident reporting focused mainly on the relevant hardware and the practices in a reporting system. These are important components, but the efficiency of a safety management system depends to a large degree on how information about risks in the system are constructed. In this study, a social construction theory lens was used to obtain a richer understanding of the behaviour of critical incident reporters and other stakeholders in a South African Air Navigation Service Provider (ANSP). This theoretical lens was then expanded by applying complexity theory to the identified socially constructed themes, in search of a richer understanding of reporting behaviour in a safety management system. Data were collected across three organisational levels: (i) the operators usually associated with the act of reporting; (ii) line managers as first-line recipients of critical incident reports; and (iii) senior-level management as strategic actors in the safety domain. The application of social construction theory highlights a critical aspect of reporting systems, showing that a sound safety management system does not depend only on the design of the system and the practice of reporting itself, as suggested by the current literature. The results show, firstly, that from an operator's perspective, the competing consequences that the system offers to a critical incident reporter are mutually exclusive and have a direct influence on the frequency and quality of actual reporting. Secondly, the results highlight the fact that each organisational level has its own socially constructed themes; some of these are similar, but others differ vastly across these levels. It is important to obtain an understanding of the socially constructed role of each organisational level and position because these roles can influence the reporting of incidents strongly. Finally, acknowledging the complex nature of the system and designing or adjusting a system based on social knowledge is pertinent in releasing the energy within the safety system. A complexity theory framework guides such insights to improving both the frequency and the quality of reporting.

**Keywords:** Critical Incident Reporting; Safety Management System (SMS); Social Construction; Complexity Theory.

[*] Corresponding author: +27837977001, jacovdw@atns.co.za

*3rd International Cross-industry Safety Conference*
*31 October-2 November 2018, Amsterdam*

# Assessment of Safety Culture from a Holistic Viewpoint: Plans, Actions and Perceptions within an Asian Airline Company

**Robert J. de Boer[3,*], David Passenier[1], Nektarios Karanikas[1], Selma Piric[1], Alfred Roelen[2], Arjen Balk[2] and Sidney Dekker[4]**
[1] Amsterdam University of Applied Sciences, The Netherlands
[2] Netherlands Aerospace Centre, The Netherlands
[3] Northumbria University Amsterdam Campus, The Netherlands
[4] Griffith University, Australia

## ABSTRACT

Safety culture is a popular concept to improve the organisational basis for safety practices in several safety-critical sectors, and aviation is internationally regarded as a forerunner. Following a request from an Asian airline company, we investigated its safety culture development plans, their implementation and the perceptions of employees, and compared these against available datasets from other aviation companies. We used the recently introduced AVAC-SCP tool to search the extent to which the organisation has institutionalised safety culture through actionable items and the degree of the realisation of these items by management. The application of the specific metric was coupled with the ASC-IT tool developed by the Netherlands Aerospace Centre for measuring safety culture levels. The ASC-IT tool was administered in a large portion of the workforce, and, to contextualise the results of both tools, we conducted 51 interviews across various company levels and functions. The findings from the AVAC-SCP and ASC-IT were compared against the data of 16 and 15 aviation companies respectively and revealed that the particular company lagged behind the industry average. More importantly, the combination of quantitative and qualitative methods allowed to picture the overall safety culture level of the organisation as well as the gaps between plans, implementation and perception within and across the different company levels and functions. Especially, the interviews offered a deeper understanding of the gaps and drove the formulation of targeted and effective recommendations for improvement. We envisage that the approach followed in this study can be applied to any organisation regardless of industry domain and comprises a systematic approach to evaluate safety culture from various angles and assist companies to gain insights into drivers and obstacles related to a mature and positive safety culture.

**Keywords:** Safety Culture; Safety Culture Assessment; Safety Culture Prerequisites.

[*] Corresponding author: +31(0) 621156269, robert.deboer@northumbria.ac.uk

*3rd International Cross-industry Safety Conference*
*31 October-2 November 2018, Amsterdam*

# Hazards in Light of Human Actions: an Autonomous Driving Challenge

**Danilo da Costa Ribeiro[1,*] and Pierre Blueher[1]**
[1]Continental Teves AG & Co. oHG, Germany

## ABSTRACT

Historically, the automotive industry was based on the assumption that one driver will be present at all times to assure the correct operation of the system. With the increase of system complexity, mostly by driving automation, the vehicle's systems began to perform some historical attributions of the driver, reducing his awareness of the vehicle's operation and, as a consequence, reducing the driver's ability to cope with some unwanted scenario. Another outcome from this increase in system's complexity is the emergence of new hazards, resulting from the higher number of interfaces between subsystems, environment and human behaviour. The development of an autonomous vehicle is even more challenging and must become more rigorous since the assumption of a driver ensuring the correct operation of the vehicle is no longer valid. To cope with such a new scenario, the safety assessment shall also keep up with this evolution and be able to detect the highest number of possible hazards and generate constraints to avoid them. Since traditional techniques are mostly focused on the system itself and do not assess properly the human interaction and environment affecting the Operational Design Domains (ODD), this work aims to evaluate how the highest number of hazards can be captured at the earliest phase of the development of a new highly automated system. Therefore, some methods were assessed to find the most compatible with this new scenario.

**Keywords:** Autonomous Driving; Functional Safety; Human Factors; Hazard Analysis; Complex Systems.

[*] Corresponding author: (+49) 69 7603 1274, Danilo.da.Costa.Ribeiro@continental-corporation.com

*3rd International Cross-industry Safety Conference*
*31 October-2 November 2018, Amsterdam*

# Developing our Skills

**Stavros Christeas**[1,*]
[1]AEGEAN Airlines, Greece

## ABSTRACT

A directive issued by the International Civil Aviation Organisation (ICAO) coming into force in 2018 requests all pilots to undergo additional training for the handling of unusual aircraft situations - known in the industry as Upset Prevention and Recovery Training. This prompted a collaboration between AEGEAN and Hellenic Air Force (HAF) which teamed up and to provide pioneering flight training to the airline's pilots. Although the directive only calls for simulated flights, AEGEAN goes above and beyond the regulatory requirements as they conduct flights in training military aeroplanes. The close-knit collaboration between AEGEAN and the Hellenic Air Force goes back many years. Several AEGEAN pilots are former HAF pilots, the two organisations have flown together at air shows, and have also collaborated on a Renegade drill, during which the HAF fighter jets intercepted an Airbus that was simulating a loss of communication. The current training programs are a result of these excellent relationships. Even though airline pilots and Air Force pilots are engaged in completely different lines of work, they share the same passion for flying and the same sense of responsibility. This explains the seamless cooperation and communication, as well as the highly professional and amicable spirit, between both sides when seated together in the cockpit. The first stage of the training procedure takes place at the HAF Aeromedical Centre. There, the AEGEAN pilots undergo hypoxia tests, which involve them being placed in a booth from which virtually all oxygen is removed, as well as simulated disorientation tests in military training equipment. The second stage involves both simulated and actual flights on military aeroplanes at Kalamata HAF base. The program is open to all AEGEAN and OLYMPIC commanders and First officers. Such a program is an unexplored area for most civil aviation pilots and is expected to benefit flight crews, and, by extension, passengers.

**Keywords:** Upset Prevention; Recovery Training; Civil and Military Aviation Collaboration.

[*] Corresponding author: +30 2103550627, Christeas.Stavros@aegeanair.com

*3rd International Cross-industry Safety Conference*
*31 October-2 November 2018, Amsterdam*

# Analysis and Evaluation of Aviation Accidents and Incidents Attributed to Incorrect Maintenance

**Thomas Gkourlias[1,*], Panagiotis Tsarouhas[2] and Anastasios Plioutsias[3]**
[1] Open University of Greece, Greece
[2] Technological Educational Institute of Central Macedonia, Greece
[3] National Technical University of Athens, Greece

## ABSTRACT

The aeroplane, a few years after its invention, began to be used as a means of public transport. Since then, the development of air transport has led both to an increase in the number of passengers per aircraft and to the aircraft size itself. Nowadays the aeroplane is considered and is one of the safest modes of transport, bringing the world together. Unfortunately, in the rare case of an aeroplane crash, the cost to human lives and society, in general, is very high. The purpose of investigating accidents is to identify their causes to prevent their recurrence in the future. Thus, among other things, the human factor and his contribution to air accidents have been thoroughly analysed, contributing greatly to their reduction. Respective investigations of the human factors involved in aircraft accidents due to incorrect maintenance of aircraft and technical staff have been done, but have not achieved their reduction to the same extent. In the present work, we initially collected, selected and recorded aviation accidents and occurrences due to maintenance errors. Then, having selected a well-recognised model (i.e. PEAR) and an established taxonomy (i.e. DIRTY DOZEN) for assessing the contribution of the human factor to accidents, we proceeded to their further analysis and categorisation. Finally, by applying appropriate statistical methods, the results were evaluated to generate proposals in the context of quality assurance and reduce maintenance-related safety events further.

**Keywords:** Aircraft Maintenance; Human Factor; Supervision; Substandard Practices.

[*] Corresponding author: tomgkourlias@yahoo.gr

*3rd International Cross-industry Safety Conference*
*31 October-2 November 2018, Amsterdam*

# Risk-based Oversight with Proactive Barrier Performance Verification

**Emma Verschoor**[1,*]
[1] Product Manager, CGE Risk Management Solutions, The Netherlands

## ABSTRACT

Bow Tie has become a well-known method that aviation organisations apply globally to perform risk-based oversight. Increasingly more airlines, airports, ground handlers, air navigation service providers and authorities are using bowties to assess risks in daily operations proactively. However, a large number of organisations tend to use bowties as a one-time risk assessment tool and archive the bowties once these are finished. Although making bowties helps organisations understanding risk scenarios and define short-term and long-term improvement actions, the creation of a bowtie costs a considerable amount of time and effort. Performing audits with the bowtie helps to avoid a static risk picture. Once the bowtie is finished and risk scenarios have been identified, barrier performance can be verified using internal audits. Questions are being asked throughout different layers of the organization. People from the top level down to the work floor answer questions about the presence and performance of barriers. It is useful to not only verify the presence of the barriers, but also the supporting activities that are linked to the barriers, such as training and maintenance programs in order to get a more complete picture. The survey results give an up-to-date risk-based oversight picture and closes the gap between paper world and real world. One of multiple organizations that adapted this method of barrier-based auditing is Fisheries and Oceans with the Fisheries and Protection Program. The bowtie presents the results in one clear overview, immediately identifying gaps between risks assessments and actual operations. This helps the Fisheries and Protection Program to make targeted risk-based decisions.

**Keywords:** Bowtie; Barrier-based Auditing; Barrier Performance; Risk Management.

* Corresponding author: +31 (0) 88 1001 350, e.verschoor@cgerisk.com

*3rd International Cross-industry Safety Conference*
*31 October-2 November 2018, Amsterdam*

# "The Future, Backwards" – a Cognitive Edge Method to Make Sense of the Context Around Complex Safety Issues

**Marion Kiely[1,*] and Friso Gosliga[1]**
[1] Cognitive Edge Practitioners

## ABSTRACT

Most safety issues are complex by nature, meaning that many correlating factors – human, technical and environmental, to name a few – play a part in any given situation. The actual safety issues are often emergent properties of such complex systems. In these circumstances, trying to design for robustness based on some ideal future state is bound to fail. Instead, we should aim for resilience, based on an understanding of the context and the dispositions within such a system. To achieve this, we need tools and methods to map and make sense of the environment from many perspectives. However, the entrained perspectives of people within an organisation often give them a limited view of the present. Such patterns of past perception can get in the way of thinking about the future. That's why Cognitive Edge developed "The Future, Backwards" as a workshop method to aid in widening the range of perspectives a group of people can take on both understanding their past and thinking about the possibilities of their future, without moving into linear scenario planning. As a creative and scalable workshop tool, "The Future, Backwards" can be used to generate prompts for further debate, to visualise and clarify different ways of thinking about safety between groups or professions within the organisation, or its data points can be used on a decision support framework like Cynefin. On the whole, the output from the exercise gives leaders an overview of the hopes and fears of their organisation around safety, helps them understand which entrained patterns of past perception are influencing the future, and provides an oblique and fun way of getting at the real issues. Participants run through the method to experience it for themselves, and then be guided through its 'inner workings'. Afterwards, people shall be able to run this in their own organisations.

**Keywords:** Narrative Based Enquiry; Sense-making; Complex Adaptive Systems Thinking; Informed Decision-making; Resilience.

[*] Corresponding author: marion@upstreamhealthandsafety.com

*3rd International Cross-industry Safety Conference*
*31 October-2 November 2018, Amsterdam*

# Aviation Safety Management Systems: a Comparative Analysis between Maintenance Steering Group (MSG-3) and Safety Management Systems (SMS)

**Lisa Whittaker**[1,*]
[1] College of Aviation, Western Michigan University, United States

## ABSTRACT

While aviation traditionally has an excellent safety reputation, new methodologies have emerged for predicting accidents and incidents. In 2010, the International Civil Aviation Organisation (ICAO) released a new initiative, Safety Management Systems (SMS). All domains within aviation will be required to implement a safety management system that complies with ICAO's guidelines set forth by member states within their regulations. The goal is to provide support for the continued evolution of a proactive strategy to improve safety performance. Aviation safety is key, but this is certainly not a new goal. Improving safety was the goal when Maintenance Steering Group (MSG) was first introduced for the Boeing 747 in 1968. The goal was to develop a system of evaluation by using decision logic of the design and maintenance of aircraft. This system was known as MSG-1. As theory evolved, MSG-2 brought process orientation and failure modes and effects analysis. Then in 1978, United Airlines, commissioned by the Department of Defense, developed a methodology based on tested and proven airline practices. With that, MSG-3 was born and has become the current standard for the industry. While MSG-3 is all about engineering and maintenance technology and SMS is more about organisational system safety, both address system safety in operations. Significant parallels exist between these two major aviation safety standards. Similarities encompass the mission of safety in aviation, the methodology of identification of hazards and analysis of risk, constituent participation (teamwork), accountability and oversight. Although MSG-3 is not a regulatory requirement, SMS is currently required by the Federal Aviation Administration (FAA) for commercial service airlines and major airports. It is also expected that SMS will eventually expand regulatory requirements to all aviation entities, but that effort has been wrought with complications. The purpose of this contribution is to compare the two programs, MSG-3 and SMS. By analysing the similarities and differences, best practices were identified. It is expected that the key points can be applied to SMS as the initiative develops.

**Keywords:** Safety Management; Aviation; Hazard Identification; Risk Analysis.

[*] Corresponding author: Lisa.whittaker@wmich.edu

*3rd International Cross-industry Safety Conference*
*31 October-2 November 2018, Amsterdam*

# Transdisciplinary Engineering in Practice: a New Buzz Word or a New Knowledge Paradigm?

**Nataliya Mogles[1*], Susan Lattanzio[1], Emily Carey[1], Alex Kharlamov[2], Linda Newnes[1], Vimal Dhokia[1] and Glenn Parry[2]**
[1] University of Bath, Mechanical Engineering, United Kingdom
[2] University of West of England, Business School, United Kingdom

## ABSTRACT

Modern engineering products are often integrated into highly dynamic socio-technical systems. The complexity of these Industry 4.0 environments which may include cyber-physical systems, the Internet of Things, Big Data, cloud and cognitive computing bring about scenarios where safety can be compromised. Maintenance of safety standards requires informed engineering design, systems thinking and collaboration with other disciplines, communities and policymakers. That is, it requires a transdisciplinary (TD) approach and knowledge formation. The concept of transdisciplinarity is not new. The origins can be traced back to 1970s when the Organisation for Economic Co-operation and Development (OECD) held a seminar in collaboration with the French Ministry of Education. Although laying the foundations for TD it was not until the 1990s, and in the face of globalisation and a rise in environmental awareness, that it gained momentum. Today, although there exists a plurality in definitions of TD at its core is to provide practical solutions to business and societal challenges by tightly integrating it within a social context. Transdisciplinarity is contrasted to Mono-, Multi- and Interdisciplinary way of working within business and academic research practices. Monodisciplinary teams work within the theoretical and methodological boundaries of a particular research field, or discipline, e.g. mechanical engineering, operations, finances, computer science, physics etc. Multidisciplinary teams combine experts from different disciplines who propose parallel solutions to the problems from the perspectives of their field without integrating discipline-specific knowledge. Interdisciplinary collaboration implies some cross-fertilisation between different disciplines where methods from one field can be applied in another research field. Transdisciplinary collaboration and thinking goes beyond the concepts of disciplines and implies a tight research integration into societal needs, values and policies. The majority of papers extracted from the SCOPUS database with the 'transdisciplinary' term are related to sustainability and health topics, and the usage of this concept in a safety domain is somewhat limited. The TD approach can be a natural method for safety assessment and design of complex socio-technical and industrial cyber-physical systems. Transdisciplinary collaboration can be realised by including the following participants within a transdisciplinary safety analysis and design team: traditional safety domain experts and specialists; newly applied disciplines, such as information technology and software engineering; policymakers, business managers, social scientists, social workers or community stakeholders; culture and societal values experts traditionally represented by humanitarians, such as anthropologists, ethics experts, artists and designers. The TD paradigm is a practical realisation of systems thinking approach towards knowledge and solutions production to complex problems with the help of the inclusion of open-minded experts from very different disciplines. Given the diversity and the number of experts within the transdisciplinary teams, new challenges of coordination and communication emerge, however, the gains acquired in delivering of new practical solutions to complex designs for safety will compensate the resources used. TREND project team funded by the British Engineering and Physical Sciences Research Council (EPSRC) will work on industrial case studies to develop transdisciplinary skills of engineers while solving resilience and safety-related problems.

[*] Corresponding author: +44 7535804981, n.m.mogles@bath.ac.uk

**Keywords:** Transdisciplinary Teams; Design for Safety; Engineering Products; Cyber-physical Systems.

*6th European STAMP Workshop & Conference*
*31 October-2 November 2018, Amsterdam*

# The Contribution of Causal Analysis Using System Theory to the Analysis and Prevention of Serious Incidents in Clinical Research Involving Healthcare Products: Preliminary Results of its Application to the TGN1412 First-in-Human Clinical Trial

**Anthony Vacher[1,*], Myra Daridan[2], Monica Pollina[3], Francesco Salvo[4], Simon Whiteley[5] and Brian Edwards[6]**

[1] Institut de recherche biomedicale des armées, France
[2] France and European Forum for Good Clinical Practice, Belgium
[3] Pharmacoepidemiologist, France
[4] Université de Bordeaux, France
[5] Whiteley Aerospace Safety Engineering & Management Limited, United Kingdom
[6] NDA Regulatory Science Ltd and Alliance for Clinical Research Excellence & Safety, United Kingdom

## ABSTRACT

In clinical research, ensuring the safety of volunteers that participate in clinical trials involving healthcare products (drugs, medical devices) is a major priority, especially when healthy volunteers choose to enter Phase I (first-in-human) trials. In that respect, in a recent joint statement from individual pharmacology and clinical professionals, they argued that incorporating the principles and methods from systems theory and human factors into the process of safety investigations following serious incidents occurring in clinical research would improve this process, and thus enhance confidence in volunteer safety. In this perspective and to illustrate the added value of systems theory and human factors methods over that already in place in human clinical research, we have applied Causal Analysis using System Theory (CAST) to a life-threatening series of adverse events that occurred during the first-in-human trial of Tegenero Immuno Therapeutics' TGN1412 in March 2006 in London (UK). The TGN1412 was a monoclonal antibody targeting leukaemia and autoimmune diseases. All six of the first healthy volunteers who received this drug experienced severe and life-threatening adverse reactions with multi-organ failure that required treatment in an intensive care unit. Following this serious incident, extensive investigations were launched by several stakeholders to identify its root-causes and propose remedial actions to avoid its recurrence. Despite these in-depth analyses and their resulting remedial actions, further fatal and life-threatening adverse events continue to occur, such as the one involving another medicinal product during a first-in-human clinical trial, this time in Rennes (France) in January 2016. This new serious adverse event has led members of the pharmacology community to question the effectiveness of the current methods used in investigations and propose the evaluation of methods used in other high-risk sectors, such as systems theory and human factors approaches. Our analysis of the TGN1412 serious incident with CAST was based on the data collected during investigations that have followed this serious adverse event and that were subsequently made available in official regulatory inspection reports. These data were expanded by information gathered from the scientific articles that have been published on the topic, and from experts in pharmacology and human clinical trials. Our results have highlighted the safety control structure in place to minimize the risk of harms to volunteers during first-in-human clinical trials and the weaknesses in this safety control structure that allowed the serious incident to occur. However, not all the reasons that led to the identified unsafe control actions could be explained due to the lack of information on the context in which they were carried out, in particular, the mental model of the operators at the time of the event. Our exploratory study suggests inadequate situational and

* Corresponding author: avacher91@gmail.com

contextual information in the investigation reports of serious incidents occurring during clinical trials. This supports CAST as a useful accident analysis tool that could be generalised to the systematic analysis of all serious incidents occurring in human clinical research.

**Keywords:** CAST Method; Human Clinical Research; Human Factors; Serious Incidents; Volunteer Safety.

*6th European STAMP Workshop & Conference*
*31 October-2 November 2018, Amsterdam*

# U-space: Safety and Security Analysis

**Carmen Frischknecht-Gruber[1], Christoph W. Senn[1] and Sven S. Krauss[1,*]**
[1] Zurich University of Applied Sciences, Switzerland

## ABSTRACT

New legislation regarding drones or Unmanned Aerial Systems (UAS) is currently being discussed in the EU and other regions. The European Aviation Safety Agency (EASA) plans to implement a traffic management system for unmanned aerial systems (UAS) called U-space by 2025 which is a service designed to provide safe and efficient operations of UAS. U-space shall enable the integration of unmanned aircraft with manned aircraft. Key features of U-space are: a) identification of UAS and its operator, b) mission planning and approval, and c) to handle potential conflicts between manned and unmanned aircraft. Based on a blueprint implementation in Switzerland we did a case study where we first applied STPA for safety analysis and then applied STPA-Sec for security analysis using the same control structure, especially to find potential conflicts between manned and unmanned aircraft as well as to find conflicts between safety and security. We did our analysis on an abstract level based on the public information which was online available for the U-space blueprint implementation. Our preliminary findings indicated that safety and security analysis cannot be well separated and should be analysed based on the same hierarchical control structure to find Inadequate Control Actions which we used as a more generic term for Unsafe Control Actions and Unsecure Control Actions. After this step, we did causal factor analysis according the guidance given in the literature by Leveson and Young. During security analysis it seemed that STPA-Sec has weak guidance regarding cyber-security and that more specific guidance by for example a catalogue of key phrases for cyber-security would be an advantage. As one result of the analysis we found that safety constraints to improve safety need also security considerations to maintain safe operation which requires a recursive approach; in our example we propose that the U-space operator may take over control of the UAS to bring the UAS out of forbidden zone in case of an emergency and the operator is not responsive to follow the instructions. That new introduced remote control needs to be properly analysed for security in order not to introduce new possible attack surfaces. We believe that a holistic systemic analysis approach will result in better system design because system properties like safety and security needs to be carefully balanced. As we based our analysis on the U-space blueprint implementation we hope to raise the awareness of the designers and regulators for these issues for the final implementation of U-space.

**Keywords:** STAMP; STPA; STPA-Sec; U-space; UAS; Drones.

[*] Corresponding author: +41 58 934 47 87, svenstefan.krauss@zhaw.ch

*6th European STAMP Workshop & Conference*
*31 October-2 November 2018, Amsterdam*

# CAST Analysis of UK Pregnancies Reported during/after Isotretinoin Administration. Proposal for Application in a Global Safety Study

**Sophia Trantza[1,*], Brian Edwards[2], Ioannis Dokas[3] and Sherael Webley[4]**
[1]University of Hertfordshire, United Kingdom
[2]NDA Regulatory Science Ltd, United Kingdom
[3]Democritus University of Thrace, Greece
[4]University of Hertfordshire, United Kingdom

## ABSTRACT

Isotretinoin, a retinoid derivative of Vitamin A, is a drug first authorized in the US in May 1982 as an oral capsule formulation with an indication for treatment of severe recalcitrant nodular acne. Within a year of its authorization in the US, it became apparent that exposure to isotretinoin during pregnancy carried a greatly increased risk of foetal malformation. Numerous traditional approaches to minimize this risk based on the label and educations have failed to adequately stop women becoming pregnant when using this medicine. Several attempts, based on pregnancy prevention programs (PPPs), have helped reduce the number of pregnancies in women receiving retinoids by mouth, but the number of pregnancies remains unacceptably high. Indeed, a recent analysis of the effectiveness of PPPs supported the widespread suspicion that they are not being followed in practice and that there is enormous inconsistency globally. Because isotretinoin is a valuable medicine for disfiguring acne, there is a need to intensify efforts to control pregnancy in exposed women and develop a common model which can be understood and applied internationally. The aim of this original research was to apply Causal Analysis using System Theory (CAST) based on Systems Theoretic Accident Model and Processes (STAMP)[1]to analyze the spontaneous events of pregnancies that have reported during or after the administration of isotretinoin the UK. The overall goal is to determine whether the results tha twill emerge from the CAST canbe extrapolated into possible new suggestions for re-designing the systemtohelp manage complex safety concerns in the future. The post-authorization spontaneous cases were obtained from the EudraVigilance database of the European Medicines Agency (EMA) via the Medicines and Healthcare Products Regulatory Agency (MHRA). The data concerned cases of pregnancies that had been reported to the MHRA in the United Kingdom during the period 01 January 2005 to 30 September 2017. The results revealed important unsafe control actions of the controllers and some failures of the physical component of the system.Based on the unsafe control actions that were found, recommendations were provided in a two way character: some changes in the Pregnancy Prevention Program with several recommendations for the controllers of the system. CAST revealed important failures and system complacency across the different levels. The easy application of CAST might well be an important way for investigating systems future failures concerning teratogenic drugs and pregnancy cases and of course other case studies in other drug cases.

**Keywords:** Isotretinoin; Foetal Malformation; Pregnancy Prevention; CAST Analysis.

[*] Sophia Trantza: +306972208166, xodouli@hotmail.com

*6th European STAMP Workshop & Conference*
*31 October-2 November 2018, Amsterdam*

# Appling STPA for a Systematic and Systemic Hazard Analysis and Management Process for the Concept Design Phase of an Autonomous Vessel

**Osiris A. Valdez Banda[1,*], Sirpa Kannos[2], Floris Goerlandt[3], Pieter H.A.J.M. van Gelder[4] and Pentti Kujala[1]**
[1] Aalto University, Finland
[2] NOVIA University of Applied Science, Finland
[3] Dalhousie University, Canada
[4] TU Delft, The Netherlands

## ABSTRACT

Recent progress in the development of technologies enabling autonomous systems has fostered the idea that autonomous vessels will soon be a reality. However, before the first autonomous vessel can be released into her actual context of operation, it is necessary to ensure that it is safe. This represents a major challenge as the experience of autonomous ships is limited. This study highlights the need for elaborating a systematic and systemic hazard analysis since the earliest design phase of an autonomous vessel. In particular, it applies STPA for elaborating an initial hazard analysis and management that provides coherent, transparent and traceable safety input information for the design of an autonomous vessel. The process is applied to analyse the hazards of two autonomous vessel concepts for urban transport.

**Keywords:** STPA; Hazard Analysis and Management; Autonomous Vessels; Safety Management Strategy.

[*] Corresponding author: +358453571182, osiris.valdez.banda@aalto.fi

*6th European STAMP Workshop & Conference*
*31 October-2 November 2018, Amsterdam*

# Review and Comparison of Modelling Approaches and Risk Analysis Methods for Complex Ship System

**Sunil Basnet[1,*], Osiris A. Valdez Banda[1] and Pentti Kujala[1]**
[1] Aalto University, Finland

## ABSTRACT

This research reviews modern modelling approach known as System Modelling Language (SysML) and risk analysis method known as Systems-Theoretical Process Analysis (STPA) and compare them against widely used traditional methods known as Tree classification method and Fault Tree Analysis (FTA). SysML is a graphical modelling language which presents system's structural composition, component functions, system's behavior, constraints and requirements. SysML aims to support the analysis, specification, design, verification and validation of complex systems. STPA is a risk analysis method which aims to identify and mitigate risks in a complex system. Unlike traditional methods such as Fault tree analysis (FTA), STPA focuses on risks due to unsafe control actions and component interactions. Furthermore, STPA can be also used in early phase of system development process to generate safety constraints and requirements for safer design of the system. SysML and STPA with the support of the RM Studio tool are applied in a workshop with Rolls Royce where ship complex systems are modelled and preliminary assessed to represent the advantage of the outcome on the application of these methods against traditional methods highly implemented in the industry.

**Keywords:** STPA; SysML; Risk Analysis; Autonomous Vessels; Ship Complex Systems.

[*] Corresponding author: +358451812811, sunil.basnet@aalto.fi