

ISSC '08 Tutorials, Workshops and Panels (as of July 22, 2008)

This year's conferences features a rich set of tutorials, workshops and panels. As you can see from the schedule below, the majority of the tutorials are planned for Monday August 25 and Friday August 29. Most of the tutorials will have prepared handouts. A few additions to this list are expected within the next few weeks.

TBD

Maintaining Safety in a COTS/GOTS/NDI Environment (Tutorial), Warren Naylor (Northrop Grumman Corporation), TBD

The COTS (COTS, GOTS, and NDI) revolution came about as a result of acquisition reform and has continued to gain momentum ever since. The original thesis was that COTS would reduce system development costs and bring products to deployment quicker with less problems. The reality has never fully achieved these benefits; however there have been some successes along the way that has resulted in the sustainment of this effort. These successes were not without sacrifices and valued lessons learned that will be passed along in this class. The main issues of COTS remain, for example, obsolescence, ruggedization, lack of development artifacts like test reports, source code, architectural structure, interrupt structures and timing, etc. These issues can be managed and a safe system can be built, however the model and methodologies used are different and the system safety engineer as well as the program's development team will have to think outside the historical verification and development models to ensure the safety of the system is acceptable and can be ultimately certified and maintained throughout the intended life cycle of the system in its intended environment. Additionally, this course will guide the system safety practitioner in dealing with unrealistic program expectations and provide them with enough forethought to adequately bid the system safety program correctly to ensure a safe system is built and maintained.

Monday - August 25, 2008

System Safety 101 (Tutorial), Rene Fitzpatrick (Raytheon Missile Systems) and Jean S. Sauerman (Raytheon Missile Systems), 8am to 4:30pm

Intended for relatively new system safety engineers, this tutorial will present the development and implementation of a fictitious system safety program from a contractor's perspective. It is intended to give the audience members an appreciation of each of the major tasks required for a successful US DOD product.

Safety-Critical Systems Design and Evaluation: Transferability of Methods Between Aviation and Healthcare (Workshop), Svetlana Taneva (Swiss Federal Institute of Technology - ETH Zürich), Effie Law (Swiss Federal Institute of Technology - ETH Zürich) and Avi Parush (Carleton University), 8am to 4:30pm

Aviation and healthcare are two prominent safety-critical domains, sharing many similarities yet differing on several dimensions. Previous work has demonstrated the likeness between airplane cockpit and operating rooms, but also the differing communication styles in the two environments. System design and evaluation methods proven effective in reducing errors and accidents in aviation may be applicable to healthcare, or vice-versa. Consequently, reusability of knowledge and skills between the domains can facilitate system safety. Given these benefits, the transferability of design and evaluation methods across these two domains is important to explore and exploit.

The goal of the workshop is to explore transferability of methods, as related to safety requirements and error factors, through a systematic review of similarities and differences of existing design and evaluation methods in both domains. Contributions from practitioners and researchers working in one or both fields are invited. Participants will engage in dialogues to reflect on strengths and weaknesses of a repertoire of methods, and how gaps between requirements and methods can be bridged with knowledge borrowed from the related domains. Follow-up activities will be organized to extend participants' efforts and interests to pursue long-term goals (e.g. developing a generic framework).

Additional details can found at <http://www.tik.ee.ethz.ch/~tanevas/ws/>

STAMP and STPA: A New Approach to System Safety for Complex, High-Tech Systems (Tutorial), Nancy Leveson (Massachusetts Institute of Technology), 8am to 2:30pm

Most of the common hazard analysis techniques used today date back to the 1950's and 1960's, with little change in the intervening years. These traditional techniques are being overwhelmed by the increasing complexity of the systems we are building today, by the introduction of digital technology and software, and by the increased reliance on distributed human-machine decision-making and control. In this tutorial, you will learn about a new model of accident causation (STAMP) and the new powerful approach to hazard analysis built upon it called STPA that allows handling much greater complexity and the new types of technology (including software) common today. It also has the ability to consider the social and organizational factors ("safety culture") factors in accidents and incidents along with the technical. STAMP and STPA apply in the early concept development stages of projects and can be used to drive the design rather than simply evaluate it afterward. STPA is being used successfully on complex systems today. The tutorial will cover fundamental principles as well as examples and experiences using the new approach.

Risk-Informed Asset Management and Optimization (Tutorial), Shuwen "Eric" Wang (ABS Consulting Inc.) and Farzin Rabii Nouri (ABS Consulting Inc.), 8am to 11:30am

In the tutorial, the general topic "Risk-informed Asset Management and Optimization" will be discussed and a tool to implement such goals is demonstrated through examples and discussions. In first section of the tutorial, the theory and the methodology used in the software are discussed briefly followed by the discussion of characteristics of the RIAMEX software. In Section 2 - "Application of the model/software", input and output information needed for the software is discussed. The audience will be guided through the Risk-informed Asset Management (RIAM) process and understand the RIAM procedures and its benefits. In the third section, an example is given to demonstrate how the RIAMEX software is applied to some RIAM case studies. This includes the data extraction technique, state definitions and the reliability performance as well as the financial performance for given maintenance strategies. The results generated by the RIAMEX software are presented and discussed to help make maintenance decisions. Through the example, the audience will get general ideas when and where the software can be applied and what information the software can provide as a tool for asset management. The areas of application and other general questions are discussed at the last section of the tutorial.

Hands-on System Safety Basics, Focused on FHA (Tutorial), Werner Winkelbauer (Frequentis AG) and Gabriele Schedl (Frequentis AG), 8am to 11:30am

An overview of a generic safety process, best suited for small to medium sized projects, in relation to the project lifecycle, is given. For each major project phase the respective safety process phase, safety objectives, necessary in- and outputs are detailed. Some state of the art analysis techniques are explained. Special emphasis is put on the Functional Hazard Assessment, where a practical guidance for a Functional Failure Modes and Effects Analysis is presented. The content of this tutorial is based on experience from an Austrian based, international working company.

Using Discrete Event Simulation for Safety Analysis (Tutorial), Sarah Sedgwick (Control Systems Analysis), 1pm to 4:30pm **CANCELLED**

Safety engineers have long recognized modeling and simulation as an essential means to portray system and process understanding. A well-developed model can assist analysts with requirements analysis, trade-off analysis, fault analysis, root cause analysis, what-if analysis and performance assessment (just to name a few). Unfortunately, as systems grow more complex, the ability to create a full-scale prototype model for engineering purposes becomes cost prohibitive. For the past 20 years, CSA has been using discrete event simulation as an affordable alternative. Discrete event simulation is a modeling methodology in which system operation is represented as a predefined sequence of events. Each event occurs at an instance of time and marks related changes to the state of the system. For the safety engineer, this type of simulation can be used to combine the system safety requirements model and the architecture model to provide a complete snapshot of the developing system and the safety positive measures being used for hazard prevention. This tutorial will address how to use

discrete event simulation for safety analysis and how this same model can effectively be used throughout the system life-cycle.

Safetykey: A Scalable Systems Safety Analysis Model (Tutorial), Matthew E. Weilert (Systems Thinking Institute LLC), 1pm to 2:30pm

The Scalable Systems Analysis model is a flexible and powerful component solution which brings several important improvements to System Safety Analysis: Structured Formal Process, Sortable Shorthand, Traceable Decision Pathways and consistently flexible scope (Scalability). One of the challenges of system safety has been the deep background required to operate effectively as a safety engineer or analyst. Structurally speaking, examples from areas as diverse as software and health care point to the fact that system improvements in the way "safety happens" require mechanizing a greater portion of the process, without losing the human intuition along the way. This contradiction now has a name: Safetykey. Through a robust five-part nested question sequence, targets of staggering complexity can be methodically analyzed (thorough yet efficient). That said, the model continues to mature, yet it needs your input to uncover its gaps so that we can all benefit from the improved process that results.

Tuesday - August 26, 2008

Essential Safety Management Tools: Threat and Error Management and the Normal Operations Monitoring (Tutorial), Chris Henry (The University of Texas at Austin) and Greg Down (Nav Canada), 1:30pm to 5pm

The Threat and Error Management (TEM) framework focuses on the operational context and how personnel discharge their duties within that context. While TEM has been developed and widely applied in aviation (flight operations and air traffic control) it is thought to be widely applicable in numerous safety-critical industries. This tutorial will focus on TEM and its use as a training, analytical, and data collection tool.

Bringing Discipline to Our Discipline (Panel), Saralyn Dwyer (APT Research) 1:30pm to 5pm

Knowledgeable practitioners of system safety engineering have been invited to make presentations of cutting-edge innovations in the practice of the discipline. Topics will include, e.g., establishing better standards of practice, and developing and applying new analytical techniques. Following each presentation, key points will be discussed by panel and audience members.

Wednesday - August 27, 2008

Introduction to Structured Qualitative and Quantitative Fault Tree Analysis (Tutorial), Joseph G. D'Ambrosio (GM Research and Development), Barbara J. Czerny, (Delphi Corporation), Rami Debouk (General Motors Research & Development), 8am to 11:30am

The tutorial will provide a basic overview of fault tree analysis. The following topics will be covered: introduction, history of FTA, FTA vs. DFMEA, Potential applications of FTA and comparison with other problem solving methods, fault tree symbols, cut sets, analysis methodology using structural and functional relationship diagrams to provide a structured approach to fault tree development, rules, common questions, quantitative analysis (including incorporation of warranty analysis and reliability prediction methods).

Lessons Learned the Hard Way - System Safety Failures in Transportation Occurrences (Tutorial), Maury W. Hill (Maury Hill and Associates), 8am to 11:30am

Given the intensive investigations often applied to them, major transportation occurrences can provide significant insights into failures of safety-related systems. The tutorial will provide synopses of selected major air, rail and marine occurrences drawn from the Transportation Safety Board of Canada. Participants will then engage in discussions with a view to identifying the safety deficiencies and inferring general lessons learned with respect to system safety.

Workshop: New Partners for Surgical Safety (Workshop), Peter Doris (Surrey Memorial Hospital), 10am to 11:00am

Our participation in the American College of Surgeons - National Surgical Quality Improvement Program (ACS-NSQIP) delivers risk adjusted statistically valid 30 day postoperative outcomes of our surgical patients. The ability to identify strengths and weaknesses of a program and to continuously measure the effects of changes in structures and processes of care, results in a commitment to embrace continuous quality improvement and new concepts for surgical safety. Consequently we partnered with : "Safer Healthcare Now" for surgical site infection prevention; an aviation expert for Crew Resource Management, briefings/debriefings, and human factors training; the World Health Organization for preoperative checklists; and a collaborative of local hospitals to spread safety initiatives. ACS-NSQIP also collaborates to identify the practices of high performing hospitals worth emulating. We will present for consideration our progress to date in these areas and demonstrate the performance of preoperative briefing and a our vision of "An Integrated Surgical Safety Management System".

Engineering Management Techniques for Complex Safety Systems (Tutorial), Michael Allocco (FAA), Dev Raheja (Design for Competitiveness, Inc.), 1:30pm to 3pm

Complex systems are an integration of several systems that result in thousands of interactions. Tweaking one portion of the system without knowing the impact on interactions is bound to create new risks of high severity. There are many unknown hazards that go unnoticed in current complex systems, which show up as product recalls roughly three per week. Such complex systems require extensive knowledge and the right execution at the right time. This paper covers the techniques of simplifying the systems to control complexity. It covers the lessons learned during the author's 30 plus years experience on complex systems such as Baltimore Mass Transit System, aircraft systems, weapon systems, hybrid electric vehicles, medical systems, and electric power systems.

Aggregating System Safety from Measures of Individual Components for Aircraft, Manufacturers, Airports and other Large Conglomerates, Alex Richman (AlgoPlus Consulting Ltd) and Leonard C. MacLean (Dalhousie University), 1:30pm to 3pm

System safety analyses are usually applied to individual components of the entity. System safety analyses for an aircraft focus on systems, components or parts. System safety assessments for a manufacturer focus on systems, components or parts for one model. It has been difficult to "connect the dots" to aggregate the analyses into a single metric for the model or manufacturer or an airport. This tutorial describes our approach to aggregating these individual system safety analyses. We discuss data base requirements, describe our analytic rationale and detail our approach. We give examples from a comprehensive aviation risk management system which includes manufacturers, aircraft models, airport and air traffic management systems.

Thursday - August 28, 2008

ISO 26262 Automotive Functional Safety Standard (Tutorial), Joseph G. D'Ambrosio (GM Research and Development), Thursday 8am to 9:30am

The tutorial will provide a basic overview of the automotive ISO 26262 functional safety standard. The standard is intended to be the sector specific version of IEC 61508 for the automotive industry, and is currently planned to be released as an ISO standard around 2010. The following topics will be covered: management of functional safety; concept development phase; product development phases: system, hardware, and software; production and operation; supporting processes; analysis methods.

Predictive Event-Sequence Analysis (Tutorial), Ted W. Yellman (Boeing), 8am to 9:30am

Predictive Event-Sequence Analysis is an innovative but little-known method which has nevertheless been used very successfully to analyze the safety of well over a hundred engineered systems mostly in commercial airplanes. (The "other" Event-Sequence Analysis—Retrospective Event-Sequence Analysis—identifies possible causes of past accidents in order to directly identify candidate safety improvements). Predictive Event-Sequence Analysis is based upon the simple principle that each undesired event that occurs during a mission must first arise at a specific time. The various possible sequences in which undesired events (which the author calls "yeweese") could arise, and their probabilities (conditional upon previous yeweese), are illustrated on an Event

Sequence Map. Predictive Event-Sequence Analysis overcomes many of the shortcomings of fault tree analysis and Markov-chain analysis—notably their difficulties in generally, clearly, and rigorously accounting for possible common-external-cause and cascading/induced yewee pairs. Predictive Event-Sequence Analyses are extremely practical and more "intuitive" to compose and to understand—and can be created without using a specialized computer program. Three simple (and always conservative) approximations for easily calculating time-dependent probabilities are developed. The author also compares the events, logic, and probability phases of the three prominent analysis methods, making this presentation a good introduction to risk analysis generally.

Joint Software Systems Safety Handbook Is Finalized (Tutorial), Archibald McKinlay (Naval Ordnance Safety and Security Activity), Peggy Rogers (Naval Ordnance Safety and Security Activity), David J. Shampine II (Naval Ordnance Safety and Security Activity), Steve Mattern (QinetiQ- North America) and Dr. Janet Gill (NAVAIR), 3:30pm to 5pm

The finalized Joint Software Systems Safety Handbook (JSSSHdbk 2008) will be presented for industry review. Interested parties can download the file before the conference and submit comments before the presentation. The update was a draft Guidebook last year, now fully formatted as a Handbook. New to this version are "Programmable Devices Safety", Systems-of-Systems Safety, and Middleware Safety.

Improving Patient Safety- What Can Be Learned from High-Risk Industries? (Tutorial), Irène K. Tael (The Royal Institute of Technology, Sweden), 3:30pm to 4:30pm

The tutorial will give the approach used, in a recently developed education, regarding patient safety. You will learn about the content and, how the lessons learned from high-risk industries, have been utilized in the development of; "Patient Safety – Theory and Implementation" at The Royal Institute of Technology (KTH). The tutorial will be based on my personal reflections, when moving from the nuclear sector to the health care sector, in Sweden. The tutorial will highlight some of the contrasts in creating safety in the nuclear field and other high-risk industries, versus the health care domain. The improvement of safety in areas where safety has been managed more explicitly, based on research, can be useful also in other domains, which you will hear about. How the history of an industry, as well as the culture, have implications for safety, and how safety is perceived, will also be covered in this tutorial. The tutorial will end by discussing how the course has been received by the "students" – the health-care professionals - and some concluding remarks.

Friday - August 29, 2008

Software Safety (Tutorial), Jonathan McNeil Sr., (US Army AMRDEC Software Engineering Directorate) and Willie J. Fitzpatrick Jr., (US Army AMRDEC Software Engineering Directorate), 8am to 4:30pm

This tutorial is an introduction to software safety. This tutorial addresses the key aspects of an effective software safety program and how to integrate these efforts into the overall program. This tutorial provides a basic understanding of System Safety and introduces the attendee to basic software safety terminology, analysis techniques, and guidelines. Emphasis is placed on developing a proactive software safety approach from the very earliest planning phases of a development project (which may include writing a Request for Proposal and Contract SOW) through product development, use/fielding and maintenance. Topics will include: System Safety Overview; Software Safety Process; Software Safety definitions; Software Safety Criticality Assessment; Software Safety planning; System Safety & Software Safety Analyses; Key Software Development Processes Activities for safety critical systems; and Software Requirements, Design, Code, and Testing guidelines for safety critical systems.

A Hands-on Introduction to System Safety Engineering (Tutorial), Laurent Fabre (Critical Systems Labs, Inc.) and Josip Pajk (Critical Systems Labs, Inc.), 8am to 4:30pm

In this tutorial, participants have an opportunity to participate in a series of key steps in the safety analysis of a software-intensive system. The tutorial is based on an example that originally created in 2004 for the U.S. Software System Safety Working Group Workshop (<http://sunnyday.mit.edu/safety-club/workshop4/>) at The Massachusetts Institute of Technology. A sample portion of the tutorial material from this 2006 presentation of this tutorial at ISSC '06 may be found at <http://www.criticalsystemslabs.com/abqtutorial.htm>.

Systems-of-Systems Safety, Artifacts, Hazard Analyses and Test (Tutorial), Archibald McKinlay (Naval Ordnance Safety & Security Activity), 8am to 11:30am

This tutorial builds on last year's half day presentation of the integrated hazard analyses, tests, and artifacts required to claim completeness for safety. This update will include stakeholder, interface, architecture, and traffic. Some contract language will be introduced. The Systems Engineering, Software Architect, and Operational Test views will be introduced.