SYSTEM SAFETY SOCIETY

Organized 1962
Incorporated 1973

Professionals Dedicated to the Safety of Systems, Products & Services

March 2008

Newsletter

The System Safety Society

Eastern Canada Chapter

Ottawa, Ontario, Canada

http://www.russona.com/ECC-SSS
www.system-safety.org

Chapter Executive

President
Robert Fletcher

Vice-President
Dave Mohan

Secretary
Raj Rao
Transport Canada

Treasurer
Gerry Einarsson
NAV CANADA, Retired

Executive Advisor
Russ McDowell
Russona Consulting

Ottawa Chapter:
http://www.russona.com/ECC-SSS/

System Safety Society
http://www.system-safety.org/

International System Safety Society Conference #26 - Vancouver 25- 29 August 2008

This year's conference will be held in Vancouver.
Web Site:
http://www.system-safety.org/~issc2008/

Dr. Jeff Joyce is the General Conference Chair. This is a "virtual conference" so although many of the members of the Organizing Committee are from Canada there many who come from throughout the USA. Volunteers are still needed during the conference with hosting speakers and registrants and setting up for presentations. If you would like to get involved, please contact Jeff at <jeff.joyce@cslabs.com>.

We have an exciting list of guest speakers.
Invited speakers include Canadians Kathy Fox of the Transportation Safety Board and Linda Keen, M.Sc., most recently President and CEO of the Canadian Nuclear Safety Commission.
From Europe we have Erik Hollnagel, a Professor and the Industrial Safety Chair at École des Mines de Paris (France).
From the United States we have Dr. Richard Cook a physician, educator, and researcher at the University of Chicago with interests in the role of technology in human expert performance, and patient safety.
Another American, Nancy Leveson, a Professor of Aeronautics and Astronautics and also a Professor of Engineering Systems at MIT will round out this group of internationally recognized experts.

System Safety Presentation: Friday, May 23, 2008

Title: Merging Assurance and the Capability Maturity Model Integration for Software: Efforts and Opportunities

Date & Time: Friday, May 23 at 11:45 am
Cost: FREE!
Location: 330 Sparks Street, Ottawa
Transport Canada, Tower C, Lower Food Court
Conference Rooms Baddeck – Vittoria St. John (FC - 29/30)

Abstract:
This presentation will examine and compare approaches taken by several organizations to align assurance-related

practices with the Capability Maturity Model Integration (CMMI) of the Carnegie Mellon, Software Engineering Institute (SEI). Here, assurance is defined to include safety, security and reliability. Although the specifics of such efforts differ, the objectives are the same: 1) to increase the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its lifecycle, and that the software functions in the intended manner 2)to promote and augment the understanding and implementation of assurance practices as critical success factors in building high quality systems for customers, and 3) to facilitate the eventual fusion of assurance-related practices with the CMMI.

Presenter: Charles Muniak, Lockheed Martin USA

Charles Muniak Ph.D. CSP is the Product Safety Officer at Lockheed Martin MS2, Syracuse, New York. He has for the last 23 years worked in several areas: system and software safety, acoustics, target motion analysis, data fusion, neural networks and management. Dr. Muniak is a member of the US Navy Software System Safety Technical Review Panel and holds two US patents for submarine localization algorithms. He holds a Ph.D. in Physiology (Biophysics specialization) from the State University of New York, Upstate Medical University, a BS in Electrical Engineering from Syracuse University and a BS in Biology from Binghamton University

Schedule:
11:45-12:00 Registration on arrival at the entrance
12:00-12:15 Opening Remarks and Introduction
12:15 - 13:00 Presentation, Questions and Answers, Concluding Remarks
13:00 – 13:30 Networking and Depart
Date: May 23, 2008
Place: 330 Sparks Street, Ottawa

Transport Canada, Tower C
Conference Rooms Baddeck – Vittoria St. John (FC - 29/30)

The final ECC presentation will take place in June with Justice Moshansky of the Dryden Inquiry. Watch for details.

Book Reviews- New books and old Books
Hollnagel, E. (2004). Barrier Analysis and Accident Prevention. Aldershot, UK: Ashgate
Rolt, F.T.C. (1960) Red for Danger London, UK: Pan Books Ltd

As Erik Hollnagel is one of the featured speakers at the ISSC in Vancouver, I thought I should become more familiar with some of his work and chose a book that discusses functional resonance in terms of accidents. The older book, Red for Danger, discusses numerous railway accidents and the improvements that were recommended but not always taken to improve rail safety.

Barriers and Accident Prevention looks at classes of accidents in order to draw lessons from these accidents. The purpose is to prevent further accidents.

One definition of resonance is an oscillation induced in a physical system when it is affected by another system that is itself oscillating at the right frequency. For example, a swing will swing to greater heights if each consecutive push on it is timed to be in rhythm with the initial swing.

Hollnagel explains the systems that are acting on each other in this systemic model. These are the four areas that contribute to accidents.
Human Performance Variability- One of the main sources of variations in performance is the Efficiency Thoroughness Trade Off, where in order to complete tasks on time or within cost, some thoroughness is sacrificed.
Technological Breakdowns due to inadequate maintenance, design flaws, etc
Latent Conditions such as a deficient safety culture or unclear indications of failures
Impaired or missing barriers.
On their own, none of these would cause an accident but occurring together they increase the “oscillation” so that an accident does occur. This theory breaks free from the linear accident model, in that

all these factors are occurring all the time. This model does not try to predict accidents. However with expert knowledge of a system, there is an opportunity to identify where accidents are likely to occur in a system. To protect against the unwanted results of an accident we can use barriers and work to reduce the variability of performance.

The book provides an interesting overview of other accident theories and is a useful addition to accident literature.

Red for Danger, originally written in 1955, allows the reader to glimpse the evolution of accident theory over the past 50 years.

The book groups the accidents by break downs of the trains themselves, bridge failures and other environmental problems, errors of drivers and errors of signalmen.

I expected that the accidents would be attributed to individuals with little regard to the environment. Indeed a few were explained by blaming the error of one person. "The accident was entirely due to an error of judgment on the part of the inexperienced driver…he ran in too fast, braked too late …".
Most accidents though, resulted in inquiries and these were thoughtful reviews of the various factors that were seen to have contributed. Early on there was an understanding, that equipment could be difficult to use and lead drivers to make errors. Weather could complicate the job of the signalmen and that they needed assistance in the form of better warning systems. Railway companies were criticized for not providing sufficient training These inquires resulted in recommendations for improvements. Unfortunately these recommendations apparently did not carry much force, for although they were hailed as revolutionary improvements in safety practices, many were not adopted for up to fifty years.

While this book is not new, it is a valuable tool in understanding how accident theory has changed and developed over time.

Call for Articles

Educating others throughout Canada regarding the use of the system safety process is our goal.

We welcome articles of approximately 200 words, in which you share your thoughts and experiences.

What "system" have you analysed? How did you conduct the analysis? What were the hazards you identified and the mitigation that was enacted to reduce the level of risk associated with each hazard? What safety techniques did you use? How did you measure the level of risk after the mitigation was completed?

We are also interested in receiving articles on Safety Management Systems (SMS). What is the framework or structure that was established for your SMS? What are the key policies and procedures within your SMS?

Please send your articles to Robin Rousham at robin.solange@sympatico.ca. He will review the articles and prepare the newsletter for distribution. Your help is most sincerely appreciated.