



October 2007

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
NAV CANADA

Vice-President

Dave Mohan
NAV CANADA

Secretary

Raj Rao
Transport Canada

Treasurer

Gerry Einarsson
NAV CANADA, Retired

Executive Advisor

Russ McDowell
Russona Consulting

System Safety Society Membership

We continue to reach out to people to encourage them to become members of the System Safety Society and our chapter in Canada.

President's Message

Look for Chapter messages on our web site: <http://www.russona.com/ECC-SSS>
Bob Fletcher

International System Safety Conference - 2007

The International System Safety Conference 2007 in Baltimore was a great success. Among several participants from Canada were representatives from Transport

Canada, Nav Canada, Thales Rail Signalling Solutions Inc., Canadian Transportation Safety Board, AlgoPlus Consulting Ltd., Critical Systems Labs, Maury Hill and Associates, Inc. – Adaptive Safety Concepts and DND.

Heather Henderson from NAV CANADA presented an interesting paper on "*The Requirements for Safety Oversight in an Air Navigation Service Provider*". Heather and Dr. Ann Lindeis, also from NAV CANADA, organized a workshop at which they and Maury Hill and Dr. Nancy Durbin addressed the topic of "*Safety Cultures – Is it all in the eyes of the beholder?*"

Robert Fletcher, from NAV CANADA, presented a paper called "*Total Organizational Safety*".

Robert was the International Chair for the conference, which for the first time, included presentations with a focus on system safety in specific countries. This year, the conference showcased the status of system safety practices in the Asia Pacific (Australia, Japan and Singapore) Austria, Canada, Russia, Sweden, and the United Kingdom.

Dr Jeffrey Joyce organized a workshop called "*Safety Analysis of the Canadian Automated Air Traffic System*" addressing questions pertaining to lessons learned during its development from 1990 to 2000. A member from Lockheed Corporation, who had been previously employed by Raytheon in developing CAATS, was on hand to provide feedback after which the discussion

was opened to the audience. Dr. Joyce also offered a workshop called "System Safety 101" on the fundamentals of system safety analysis.

Certification of System Safety Engineers

An area that surely will remain controversial for some time is the certification of system safety engineers.

I remember attending the SIGSOFT '91 conference in New Orleans where system safety engineer certification was raised as an issue. Little has changed since that time and I exclude, of course, the designation of Certified Safety Professional (CSP).

The expertise of those who would refer to themselves as "system safety engineers" varies substantially. We have witnessed this since our early days, analyzing the safety of the THERAC-25. We have seen some very scary examples along the way. We have witnessed this by the safety standards that have been produced. There are those who are experienced with:

- MIL-STD-882,
- IEC 61508,
- SAE ARP 4761, or
- MOD 00-56.

There are also those who have:

- Experience in system safety
- Experience in both system safety and software safety (a more rare breed also with considerable variance in expertise)
- Experience in electrical, and electronic systems and those who have experience in hydraulic, mechanical and pneumatic systems as well
- Only reviewed others' analyses
- RAM experience
- System engineering experience
- A little or a great deal of knowledge
- An over-zealous approach.

This list can go on and on. You will notice no mention of anything regarding experience in particular safety-related sectors. Our experience continues to be that many system safety engineers' expertise is built

on quicksand. Many do not pass very basic tests in terms of being able to identify what and what is not a hazard. Unfortunately, the same thing is true for failure modes. We had recent experience with a "system safety engineer" (consultant) representing the client on a multi-million dollar project where he had never heard of quantitative fault trees and was not aware of a minimal cut set.

We have also seen cases where the "system safety engineer" on projects, either for the customer or contractor, has zero experience in the field. We recently subcontracted to a system safety engineer with (apparently) 20 years experience. Once he acquired the knowledge of the system to be analyzed and it was time for the rubber to meet the road, we discovered he was incompetent at fault tree analysis. As a result, we immediately terminated his contract - a costly experience!

Our experience also indicates that many system safety engineers have no sense for "what is sufficient/acceptable". It seems that, if they have achieved this ability, they move on to other positions.

Since it depends on the knowledge of the customer, insufficient qualifications in system safety engineers often is not identified. The most successful safety-related contracts are often those where the client is capable in system safety as well as the contractor.

The need for certification is certainly evident. I believe, in the long term, certification is possible. It will of course require a group of very knowledgeable and experienced people to implement it.

Does anyone else care to comment? If so, the editors will be pleased to publish your response in the next newsletter. Thank you.

David Levan

David is a system safety and software safety engineer with 21 years experience. He was Canada's pioneer consultant in software safety, teaching safety courses for about 15 years. He was the consultant on the THERAC-25, and DND's SME on system safety for the Maritime Helicopter Program.

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

Next year's conference will be held in Vancouver.

Web Site:

<http://www.system-safety.org/~issc2008/>

Jeff Joyce is to be Conference chair, Rod Simmons is Technical Program Chair, is Publicity chair, Ann Boyer is Finance chair, and Bob Fletcher is the International Chair.

Chapter members should plan to attend. If we plan now, we should be able to write a paper to present or organize a tutorial for the occasion.

The conference will showcase Canada in a setting of system safety professionals like never before. It should be one of the best conferences ever.

It should be fantastic. The hotel is a sight to behold and, of course, Vancouver is like a diamond between the sea and white-topped mountains.

To top it off, a group of spouses is organizing an Alaska cruise that will follow the conference.

Upcoming Activity

Eastern Canada Chapter of the System Safety Society presents:

Emergency Management: The Past, the Present and the Future

Tuesday, October 30, 2007

Place: Ottawa Public Library Auditorium Metcalfe at Laurier (Auditorium is located on the Basement Level) *Schedule:*

- 11:45 - 12:00 Registration on arrival at the Ottawa Public Library entrance
- 12:00 - 12:15 Opening Remarks and Introduction

- 12:15 - 13:00 Presentation / Discussion
 - 13:00 - 13:30 Networking and Depart
- Cost: \$10 non-members, \$5 members, Students free.

We are pleased to invite everyone interested in system safety to a System Safety Society discussion at the Ottawa Public Library, Lower Auditorium on Tuesday, October 30, 2007 at noon by Michael Nolan (Chief of Paramedic Service and Director of Emergency Services for Renfrew County).

Chief Nolan will provide an overview of the current public sector Emergency Management practices in Canada. Discussion will focus on the principles of: planning, hazard identification and risk assessment, community resilience, business continuity as well as the response and recovery cycles.

Examples of recent significant events will be discussed applying these principles, such as the Ice Storm in Eastern Ontario and Western Quebec, the F2 Tornado affecting the community of Combermere in 2006, as well as anticipated threats such as an influenza pandemic. The objective of this discussion will be to:

- Promote awareness of current Emergency Management practices in Ontario;
- Empower individuals to become self sufficient in their home for up to 72 hours;
- Inform businesses and corporations of the need to establish and practice business continuity planning; and,
- Improve our societal resilience to impending catastrophic events.

Background of Michael Nolan: As Director of Emergency Services and Chief of the Paramedic Service Michael is responsible for 911 service, Fire Communications for 19 departments, Emergency Management the Paramedic Service stretching from the City of Ottawa in the East along the Ottawa River North to beyond Algonquin Park and Westerly to the boundaries of Hastings County.

Michael is visiting faculty for Public Safety Canada at the Emergency Management College in Ottawa working with senior municipal and provincial staff to better prepare their home communities in responding to major events. As a member of the Board of Emergency Medical Services Chiefs of Canada, Michael works closely with Paramedic Services across the country to share best practices and promote policy direction that aligns with the advancement of excellence in pre-hospital care.

Having worked as a Critical Care Flight Paramedic throughout Ontario, Professor of Health Studies in Prince Edward Island and as the Manager of Emergency Measures for the City of Ottawa, Michael is grounded by the knowledge that the service he and his co-workers provide every day makes a difference in the lives of his community.

We look forward to seeing you!

Ottawa Chapter:

<http://www.russona.com/ECC-SSS/>

System Safety Society:

<http://www.system-safety.org/>

Transport Canada NEWS

Transport Canada will unveil the Safety Management System Complexity Guide-SMS Guidance Material for small operators at the Flight Training Committee meeting on Sunday November 4, 2007 at the Air Transport Association of Canada AGM in Halifax Nova Scotia.

Call for Articles

As we observed last year, educating others throughout Canada regarding the use of the system safety process is our goal. Happily this edition includes an article indicating strongly a need for system safety engineer certification.

You, too, can help by sharing your ideas and your experiences from working on safety critical projects or, indeed, responding to David Levan's very interesting article in this edition.

We need articles of approximately 200 words. In which we want you to 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.