

Space Systems Risk Management Symposium



"What Works – What Doesn't"

Tutorials

The Aerospace Corporation
El Segundo, Calif.

April 6-8, 2010

Tuesday, April 6

Introduction

The 2010 *Space Systems and Risk Management Symposium* will feature a full day of tutorials focused on risk management, with sessions offered in the morning and afternoon.

Each session will feature four hours of training by leading experts from The Aerospace Corporation, NASA, and academia. Topics will include risk-informed decision making for acquisition design; risk techniques for program management and design; basic risk management planning and assessment; software reliability for quantitative assessment; and the systems engineering-risk management relationship.

The \$150 registration fee for each tutorial session includes a workbook containing copies of the presentation slides.

Tutorial Sessions

A. Risk Management and Assessment Fundamentals

Dr. Sergio Guarro, The Aerospace Corporation

B. Overview of Probabilistic Risk Assessment and Its Role in Risk-informed Decision Making

Dr. Homayoon Dezfuli, NASA

C. Using Evidence and Risk to Enable Successful System Acquisition

Dr. Barry Boehm, University of Southern California

D. Space Vehicle Reliability Engineering

Ron Duphily, The Aerospace Corporation

E. Software Technology Readiness Assessment for National Security Space Programs

Dr. Peter Hantos, The Aerospace Corporation

F. Decision Theory Applied to Quantitative Risk Management

Dr. George Friedman, University of Southern California

Space Systems Risk Management Symposium



"What Works – What Doesn't"

Tutorials

The Aerospace Corporation
El Segundo, Calif.

April 6-8, 2010

Tutorial A: Risk Management and Assessment Fundamentals

Dr. Sergio Guarro, The Aerospace Corporation

April 6, 2010

8 a.m. to noon

This tutorial covers the basic principles and underpinnings of space system risk management (RM) and risk assessment (RA). It also addresses the most common practical implementation issues that arise in complex, multi-level programmatic environments. The fundamental risk concepts covered by the tutorial include basic definitions of RM processes and models, and the most common qualitative and quantitative techniques for risk assessment and handling that may be encountered in the field.

Practical RM implementation issues covered in the course include:

- Calibration of risk classification / quantification scales
- Integration of RM processes in multi-level program and enterprise environments
- Selection of appropriate risk models and relation of programmatic RM/RA models to formal "PRA" (Probabilistic Risk Assessment) risk modeling techniques

The course discussion is supported by a number of real-life examples and by mini-case-studies.

Tutorial Instructor Background

Dr. Guarro is a Distinguished Engineer in the Systems Engineering Division (SED) of the Aerospace Corporation Engineering and Technology Group (ETG). He started his career in the nuclear industry, working for the U.S. Nuclear Regulatory Commission and the Lawrence Livermore National Laboratory. He joined the Aerospace Corporation as an Engineering Specialist and then carried several management positions, including those of Manager of the Reliability and Risk Assessment Section in the Electronic Systems Division and of Director of the Risk Planning and Assessment Office in SED.

Dr. Guarro applies his multi-decade expertise in systems engineering, risk management and mission assurance disciplines to the development, coordination and pilot implementation of processes for which the Aerospace Systems Engineering Division has technical ownership and responsibility, working across the spectrum of U.S. Government space systems and agencies. He has developed risk and mission assurance methodologies for space systems and missions of national interest, such as the EELV (Evolved Expendable Launch Vehicle) and the NASA Cassini mission, and has served on National Research Council committees as an expert panelist for space systems risk and safety assessment. His work is documented in abundant open literature publications, as well as in instructional and guidebook materials produced for Aerospace and for U.S. Government Customers.

Space Systems Risk Management Symposium



"What Works – What Doesn't"

Tutorials

The Aerospace Corporation
El Segundo, Calif.

April 6-8, 2010

Tutorial B: Overview of Probabilistic Risk Assessment and Its Role in Risk-informed Decision Making

Dr. Homayoon Dezfuli, NASA Headquarters

April 6, 2010

8 a.m. to noon

Probabilistic Risk Assessment (PRA) is a systematic approach to modeling the behavior and especially the interaction of hardware, software, human elements, and operating environment of a system, whose goal is the identification and quantification of scenarios that can lead to undesired system states. Stochastic models are employed to represent, and in some cases to identify, these scenarios. Uncertainties in models and parameters are represented with probability distributions, and this representation relies upon Bayesian inference to provide a mathematically coherent and consistent framework.

Because of the ability of PRA to quantify integral risk metrics (e.g., probability of loss of mission), it is increasingly playing a key role in risk management. The tutorial will begin with an overview of the NASA risk management (RM) approach outlined in NPR 7000.4A, including coverage of its two constituent processes: Risk-Informed Decision Making (RIDM) and Continuous Risk Management (CRM). Following this overview, we will discuss how the RIDM process is applied in the formulation phases of programs to inform decision making in selecting alternatives and establishing baseline performance requirements. In this context, the role of risk analysis in quantifying uncertainties associated with performance measures for safety, technical, cost, and schedule will be discussed. This will set the stage for the PRA presentation that will follow which discusses key PRA concepts, scenario-based accident modeling techniques using simplified aerospace examples, and PRA applications to support decision making.

Tutorial Instructor Background

Dr. Homayoon Dezfuli is the NASA System Safety Engineering Technical Fellow and Manager of System Safety in the Office of Safety and Mission Assurance at NASA Headquarters (HQ) in Washington, D.C. In these roles, Dr. Dezfuli serves as a senior technical expert in the system safety discipline within the Agency and is responsible for NASA's policies and procedures for system safety and risk management. He has been instrumental in developing and implementing advanced system safety and risk management techniques and processes for the agency, in addition to leading several major policy and technical procedure development tasks. Dr. Dezfuli has over twenty years of experience in system safety and Probabilistic Risk Assessment (PRA) applications and methodology development. He co-authored and managed the development of the NASA PRA Procedures Guide and the NASA risk-informed decision-making handbook. He has authored many papers in the areas of technical risk assessment and management. He is currently leading several high priority projects at NASA HQ aimed at institutionalizing the risk-informed decision-making process at NASA. Dr. Dezfuli has a Ph.D. in nuclear engineering from the University of Maryland.

Space Systems Risk Management Symposium



"What Works – What Doesn't"

Tutorials

The Aerospace Corporation
El Segundo, Calif.

April 6-8, 2010

Tutorial C: Using Evidence and Risk to Enable Successful System Acquisition

Dr. Barry Boehm, University of Southern California

April 6, 2010

8 a.m. to noon

Many acquisition programs fail because they commit to go forward with a set of plans and specifications for which they have little to no evidence of feasibility. This tutorial presents a DoD 5000.02-compatible version of a commercially-successful evidence and risk-based system acquisition process, illustrates its application to large DoD systems, and provides exercises for learning how best to apply it on DoD programs. Its key is to make the evidence of feasibility a first-class deliverable which is assessed by independent experts. Shortfalls in evidence are uncertainties, which when multiplied by mission criticality become risk exposures, which should be addressed by risk management plans. Acquisition managers must then decide whether to accept the risks and go forward, or to re-baseline the specs and plans or do more homework before proceeding. The tutorial will also present an Incremental Commitment process model that supports the approach, along with a set of early-warning risk assessment tools to help developers and acquirers identify and prioritize program risks before they become show-stoppers.

Tutorial Instructor Background

Dr. Barry Boehm, TRW Professor, Computer Science and Industrial and Systems Engineering Departments, University of Southern California (USC)
Director Emeritus, USC Center for Systems and Software Engineering
Director of Research, DoD-Stevens-USC Systems Engineering Research Center
B.A., Harvard, 1957; M.A., Ph.D., UCLA, 1961, 1964; Sc.D. (hon.), UMass, 2000

Dr. Barry Boehm served within the U.S. Department of Defense (DoD) from 1989 to 1992 as director of the DARPA Information Science and Technology Office and as director of the DDR&E Software and Computer Technology Office. He worked at TRW from 1973 to 1989, culminating as chief scientist of the Defense Systems Group, and at the Rand Corporation from 1959 to 1973, culminating as head of the Information Sciences Department. He entered the software field at General Dynamics in 1955.

His current research interests involve recasting systems and software engineering into a value-based framework, including processes, methods, tools, and an underlying theory and process for value-based systems and software definition, architecting, development, validation, and evolution. His contributions to the field include the Constructive Cost Model (COCOMO) family of systems and software engineering estimation models, the Spiral Model and Incremental Commitment Model of the systems and software engineering process, and the Theory W (win-win) approach to systems and software management and requirements determination. His MS-level software engineering course involves 20 teams per year in service learning by negotiating and developing useful software applications for USC campus and USC neighborhood community-service and small-business clients.

He has received the ACM Distinguished Research Award in Software Engineering, the IEEE Simon Ramo Award in Systems Engineering, and the IEEE Harlan Mills Award in Software Engineering, and lifetime achievement awards from the American Society for Quality Control and the International Society of Parametric Analysts. He is a Fellow of the primary professional societies in computing (ACM), aerospace (AIAA), electronics (IEEE), and systems engineering (INCOSE), and a member of the U.S. National Academy of Engineering.

Updated 1/21/2010

Space Systems Risk Management Symposium



"What Works – What Doesn't"

Tutorials

The Aerospace Corporation
El Segundo, Calif.

April 6-8, 2010

Tutorial D: Space Vehicle Reliability Engineering

Ron Duphily, The Aerospace Corporation

April 6, 2010

1 to 5 p.m.

Space Vehicle (SV) Reliability Engineering Tutorial – The tutorial will help to plan for appropriate reliability requirements and review activities that will improve the probability of mission success. Both government and contractor roles, responsibilities, key reliability tasks and necessary resources are described to help converge on agreements necessary for mission success. The material will review SV Reliability Figures of Merit (FOM) and how they influence systems development. It will also provide a sense of where to focus efforts to minimize failures and disconnects.

Tutorial Instructor Background

Mr. Duphily has over 42 years experience in Reliability, System Safety and Risk Assessment of Spacecraft, Laser Systems, Launch Vehicles and Nuclear Power Plants. He has been responsible for assisting Goddard Space Flight Systems (GSFC) with the development of a Probabilistic Risk Assessment (PRA), Hubble Risk Assessment as well as helping the with the completion of Fault Tree Analysis (FTA) and Failure Modes and Effects Analysis (FMEA). Author of the Risk Management, Reliability, Safety, Configuration Management and QA chapters of Space Vehicle Systems Engineering Handbook.

While at TRW he was a Department Manager responsible for Reliability, Maintainability, System Safety, Configuration Management and Data Management.

As a Reliability, System Safety and Risk Assessment consultant he assisted in the preparation of several PRA's on Nuclear Power Plants.

Programs Expertise:

2001-2009 Risk and Reliability Assessment/review on SMC, NRO and NASA programs
2000-2001 PRA lead on NASA GSFC SORCE Project and NASA Ames Design for Safety
1985-2000 TRW - TDRSS, Laser, Launch Vehicle Initiative Reliability and Safety Manager
TRW - Department Mgr. for Reliability, System Safety and Configuration Management
1980-1985 Independent Reliability, Safety and Risk Assessment Consultant on several
Nuclear Power Plant Projects: Oyster Creek, Yankee Rowe, HTGR, etc.
1968-1980 Reliability Analysis on Minuteman III, Pioneer 10, Skylab, Fltsatcom, Nuclear
Power Plants, etc.

Related Teaching Experience:

Space Vehicle Reliability Engineering Tutorial
COTS Risk Management Seminar
Internal TRW courses on Reliability and Risk Management

Degrees Received:

1966 BSME Mechanical Engineering, University of Massachusetts, Dartmouth, Mass.
1974 Certified Reliability Engineer, ASQ
1976 Registered Professional Engineer-Mechanical Engineering, Massachusetts

Updated 1/21/2010

Space Systems Risk Management Symposium



"What Works – What Doesn't"

Tutorials

The Aerospace Corporation
El Segundo, Calif.

April 6-8, 2010

Tutorial E: Software Technology Readiness Assessment for National Security Space Programs
Dr. Peter Hantos, The Aerospace Corporation
April 6, 2010
1 to 5 p.m.

A central theme of the defense acquisition process is that the technology employed in weapon system development should be "mature" before system development begins. A Technology Readiness Assessment is a systematic, metrics-based process that assesses the maturity of selected technologies, called Critical Technology Elements (CTEs) in weapon systems. The DoD in its Technology Readiness Assessment (TRA) Deskbook does offer quite substantial help on assessing hardware technologies, but with respect to software used in space systems the guidance is weak and ambiguous. Since conducting TRAs on major space acquisition programs is mandatory, gaining a better insight into this essential acquisition process is very important. Based on broad experiences stemming from the support provided to numerous programs, the tutorial's objective is to offer tangible guidance on identifying CTEs, establishing Technology Readiness Levels for space software, and to provide further insights into several, related dimensions of technology risk mitigation. The participants expected to gain familiarity with the TRA logistics context, stakeholders and their processes, and legal and compliance considerations. The participants will also learn to identify critical software technology elements, to deal with hardware-software dependencies during TRAs, to rate the maturity of software CTEs, and to understand the difference between the goals of a TRA and customary risk management practices.

Tutorial Instructor Background

Peter Hantos is a Senior Engineering Specialist at The Aerospace Corporation. In this capacity he has been supporting the US Air Force and various other government organizations on software issues related to the acquisition of space systems. Most recently, he was the software technology readiness sub-team lead on the Technology Development project of the Air Force Smart Operations 21/Developing and Sustaining Warfighting Systems (AFSO-21/D&SWS) effort. He has over 35 years of experience as a professor, researcher, software engineer and manager, and has authored numerous technical papers, U.S. and international conference presentations. Prior to joining Aerospace, as Principal Scientist at the Xerox Corporate Engineering Center, he developed corporate-wide engineering processes for the development of software-intensive systems. Earlier, as Department Manager, he directed all aspects of quality for several laser printer product lines. Other highlights of his Xerox career include the creation and management of a software technology group to facilitate the technology transfer and productization of software prototypes from the Palo Alto Research Center. He holds M.S. and Ph.D. degrees in Electrical Engineering from the Technical University of Budapest, Hungary.

Space Systems Risk Management Symposium



"What Works – What Doesn't"

Tutorials

The Aerospace Corporation
El Segundo, Calif.

April 6-8, 2010

Tutorial F: Decision Theory Applied to Quantitative Risk Management
Dr. George Friedman, University of Southern California
April 6, 2010
1 to 5 p.m.

As evidenced by the title of this symposium, risk management has become an important discipline within systems engineering to manage the ever increasing complexity of our developments. Often when risk management has been employed, it has been approached from an essentially qualitative and heuristic viewpoint. It can be argued that evolving risk management from qualitative to quantitative techniques will further enhance its utility to provide greater integrity and resilience to new programs. This tutorial develops a rigorous methodology that permits the discipline of decision theory – originally developed in the economic world – to be applied to quantitative risk management of engineering systems. Moreover, there will be a special emphasis on how testing, and the quality of testing, can be folded into the decision theoretic framework. Of necessity, some probability theory will be required in the tutorial, but it will be its most elementary aspects and the students will require no prior experience with probability.

Tutorial Instructor Background

Presently, Dr. George Friedman is the Associate Director of the Systems Architecting and Engineering program at the Viterbi School of Engineering at the University of Southern California, in Los Angeles, Calif. He has originated four new courses in engineering at the graduate level and is presently teaching two of them. Since 1995, almost a thousand students at the M.S. level have taken his courses and he has sat on 15 Ph.D. committees. His research interests include the application of decision theory to quantitative risk management and the application of graph theory to multidimensional math model management.

Previously, Dr. Friedman spent 45 years working in industry, retiring from Northrop as the corporate vice president of engineering and technology in 1993. He is a founder, third president, fellow and associate editor of the International Council on Systems Engineering (INCOSE). He is also a fellow of the Institute of Electrical and Electronic Engineers (IEEE) and served as vice president of publications for the Aerospace and Electronic Systems Society of the IEEE. He also served as a consultant to DoD, NASA, CIA, and NATO.

B.S.: UC Berkeley; M.S. and Ph.D.: UCLA