Foreword

This course is intended for a senior undergraduate or graduate engineering or science student. Some basic familiarity with nuclear power system design and operation is assumed. The objective is that the student will come away with an overall appreciation of the approach to nuclear reactor safety concepts and safety design. The focus is on concepts: the "know why" and some of the top level "know how". The details or the "know what" are glossed over.

Where examples are used, we focus heavily (but not exclusively) on CANDU®[1], for three reasons: we expect that the CANDU reactor design will be of primary interest to students taking this course; there **are** textbooks on Light Water Reactor safety; and there are **no** such textbooks on CANDU. We also use the Advanced CANDU reactor (ACR-1000) for some examples.

Nuclear reactor safety is a broad field. It is first, but not only, based on science, since in order to make something safe, you have to at least know how it works. Thus it happily uses physics, chemistry, most fields of engineering (process, mechanical, civil, instrumentation and control), and biology. Some engineering mathematical tools have been developed specifically for safety, such as Probabilistic Risk Assessment (first used by NASA to determine the likelihood and consequences of failures in space shuttles), and Safety Analysis, which predicts the response of the plant to postulated accidents - the better to design against them.

The course assumes that the student has a general engineering or science background at the senior undergraduate level, including basic calculus and probability theory, but does not assume prior knowledge of reactor physics, thermohydraulics, fuel, etc. Whenever science or engineering in these areas is needed to understand the safety concepts, it is summarized very briefly; the reader can consult the references for a more comprehensive treatment. It does however assume the student knows (or can read up about) the basic design of a CANDU reactor; the student should know the major pieces and how they work. It also assumes the student has basic undergraduate math. skills - if not, UNENE offers a free refresher course in same.

No engineered system can be made absolutely safe, whether it be a car, aeroplane, toaster, children's toy, or nuclear reactor. What society demands is the such products be made 'safe enough' or 'acceptably safe'. The definition and implementation of this goal for nuclear reactors is called 'safety philosophy', and we will cover some of its elements.

However as even a brief survey of real accidents over the past four decades will reveal, human

---

[1]Acronym for <u>CAN</u>adian <u>D</u>euterium <u>U</u>ranium, although if you don't know this, you probably shouldn't be taking the course.

errors are both the major contributor to accidents, and the major means of recovering from them. We will not cover in this course the evolving science of human behaviour, but instead will concentrate on the way the design tries to eliminate, compensate, or withstand human error.

In the end safety is as much of a state of mind as a hard science, particularly during actual operation of a nuclear power plant. Such a state of mind has been recognized as so important in recent years that a name has been coined for it: "safety culture", an attitude of placing safety first that permeates an organization.

Acknowledgements

This course was originally given by Prof. W. Garland who used his extensive knowledge of the topic and how to present it in a university setting, along with some source material from Dr. V.G. Snell and others, to create a unique product. Dr. Alan Monier, Interleaf, was involved with the course development and provided practical interpretations of the key concepts throughout. This particular version includes substantial revisions by Dr. Snell. Dr. D. Meneley's lectures on CANDU at the University of New Brunswick were also consulted and some of his excellent material was gratefully used in this revision, with his kind permission. The resulting revised course was first given in 2001. Further revisions have been made by V. Snell to the 2002, 2003, 2004, 2006 , 2008 and 2009-10 versions.

Although the Canadian nuclear industry encourages the course and is the source of a lot of the technical information, the course does not represent the views of any company nor the industry; nor do such organizations take responsibility for the material herein. As usual, any errors can be laid squarely at the feet of the authors. If you find any, let me (Snell) know.

To the best of our knowledge, all material herein is not proprietary - hard to find elsewhere, perhaps, which is one reason why the course was put together, but not commercially protected. If you find something which shouldn't be here, again, please let me know.

Expectations

The McMaster EP-714 course is composed of 13 lectures covered in 9 chapters of this textbook. The EP-714 classes run about three hours a week for 13 sessions, with a break in the middle of each class. Table F-1 below shows a typical plan for a 13-week course, although the amount of discussion and interest will (and should) change this plan as we proceed. The UNENE version covers the same material but runs typically over four alternate two-day weekends.

The student's mark on the course is determined by successful completion of the assignments, projects, tests, presentations and final exam. These are also shown in Table F-1 below and are typical. For the UNENE version, which is greatly compressed in terms of elapsed time but not in content, a revised outline (Table F-2) and a revised marking scheme are used (Table F-3) - again, these are typical. Attendance at and participation in the course is a prerequisite for passing.

Please remember that McMaster requires a 70% mark (B-) to get credit for the course. Students may work in pairs on their project, as long as the contribution of each is clearly described, and are allowed to do so on the assignments, within reason, again with each contribution delineated, where explicitly permitted by the professor. Tests and exams are done only by the individual.

Academic integrity is taken very seriously by UNENE and member universities. Students in both the McMaster diploma and the UNENE M.Eng. are strongly advised to review the mini-course on academic integrity (it is in fact a requirement for UNENE students), which can be found at http://www.unene.ca/courses/coursedescriptions.htm, with a short description and a link to the course page http://www.unene.ca/un-acad-integrity/index.htm.

In many cases the student will be able to find "official" answers to some of the exercises - i.e., the same problem may have been addressed by AECL, CNSC or a utility. Little credit will be given for relying heavily on such work, and none for reproducing it - the course emphasis is to encourage independent and logical thinking about reactor safety. And who says that the industry has the best answer anyway?

The student is strongly encouraged to read, or at least to skim, the text material beforehand. The lectures will *not* consist of reading the text but we will discuss various aspects of it. For EP-714, the student should plan on spending about 10 hours per week reading the text, completing the assignments and the project (if chosen), and attending the lectures. The UNENE format will demand more concentrated effort over the shorter period, typically 100+ hours over the 8 weeks in addition to class time. A distance education option is available for students outside the GTA.

Some of the projects require at least a superficial knowledge of FORTRAN programming or a

similar language. While this is not a computer programming course, scientific programming is part of the safety analyst's toolkit, and for better or worse, most industry codes are written in antique versions of this antique language. Public domain compilers and a free electronic book on FORTRAN are available on the Internet and one will be chosen if needed.

Table F-1 - Typical Course Plan (EP-714)

Lecture	Chapter / Major Sections	Assignment / Project / Presentation
1	**Chapter 1 - Introduction** • The Double-Edged Sword • What is the Hazard? • Effects of Radiation • How Radioactivity Can Escape • That's Incredible • Risk	Finalize course schedule, evaluation method; present & discuss possible projects
2	**Chapter 2 - Accidents** • Accident Identification • Evolution of Canadian Safety Philosophy • Single-Dual Failure Approach • Probabilistic Safety Assessment • Consultative Documents C-6 and RD337 • Other Countries / Other Designs	Submit exercises at the end of Chapter 1 (5% of total mark).
3	**Chapter 3 - Case Studies** • Reactor Physics • Criticality Accidents and Power Excursions	Submit exercises at end of Chapter 2 (5%). Student & class discussion of approaches taken. Test (5%) Decide on project.

Lecture	Chapter / Major Sections	Assignment / Project / Presentation
4	• Loss of Coolant • Power Runaway **Chapter 4 - Probability Tools and Techniques** • Definitions and Rules • The Bayes Equation • Example - Core Monitoring System • Failure Rate Estimation When No Failures Have Occurred	Submit exercises at end of Chapter 3 (5 %). Student Presentation of Exercise 2 from Chapter 3 & class discussion. Finalize Project and assign responsibility. Discuss how project is to be done.
5	• Probability Distributions • Fault Tree Example • 2 / 3 Logic Example • Ladder Logic • Unavailability Targets • Dormant vs. Active Systems	Student presentation of scope & plan of their project; class and lecturer feedback.
6	**Chapter 5 - Safety Systems** • Shutdown Systems	Test (5%). Student initial discussion of mathematical models in their projects.
7	• Heat Removal Systems • ECC • Containment & Sub-systems • Monitoring	Student final detailed written submission, presentation & discussion of project plan and scope. (5%).

Lecture	Chapter / Major Sections	Assignment / Project / Presentation
8	**Chapter 6 - Safety Goals** • Basis of Numerical Safety Goal • Derivation of Numerical Safety Goal • Other Safety Goals • Limitations of the Risk Approach	Submit exercises at end of Chapter 5 (5%). Student presentation & submission of the equations for their mathematical models (5%).
9	**Chapter 7 - Accident Analysis** • Selection of Initiating Events by Pseudo-Frequency • Categorization of Initiating Events by Phenomena • High Level Acceptance Criteria • Major Computer Analysis Tools Required for DBA • Selection of Initial Conditions • Typical Initiating Events • Large LOCA	Submit exercises at end of Chapter 6 (5%).

10	◄ Small LOCA & Single Channel Events
	   ◄ Loss of Forced Circulation
	   ◄ Main Steam Line Breaks
		Student presentation & submission of flow charts and numerical methods for their programme; selection of test cases & data (5%).

11	**Chapter 8 - Technology of Accident Analysis** • Reactor Physics • Fuel	Submit exercise at end of Chapter 7 OR test (5%); discussion of approaches taken for this exercise.
12	• Heat Transport System • Fuel Channels • Moderator • Containment • Fission products/Dispersion / Dose	Round-robin on project: progress, problems

Lecture	Chapter / Major Sections	Assignment / Project / Presentation
13	**Chapter 9 - Whither Safety?** • IAEA • International Nuclear Event Scale • INSAG & Safety Culture • INPRO • Generation IV • Evolutionary & Passive Designs • Categories of Passive Safety • Passive Safety Desiderata • AP600/1000 • Eskom PBMR • Passive CANDU	Students present & submit their final mathematical and computer models and code predictions (20%). Final exam (25%) Feedback on course - changes for next time

Table F-2 - Typical Course Plan (UNENE Format)

The technical contents and detailed subjects are similar. However the time distribution differs since the course is typically spread over four weekends:

Days 1 & 2

Chapter 1	Introduction
Chapter 2	Design Basis Accidents
Chapter 3	Part 1 - Reactor Physics

===

Days 3 & 4

Chapter 3	Part 2 - Case Studies
Chapter 4	Probability Tools and Techniques

===

Days 5 & 6

Chapter 5	Safety Systems
Chapter 6	Safety Goals
Chapter 7	Accident Analysis

===

Days 7 & 8

Chapter 8	Technology of Accident Analysis
Chapter 9	Whither Safety? International Trends
Appendix	Glossary & Acronyms

Test

Table F-3 - Typical UNENE Marking Scheme

1st test	1st home-work	2nd Test	2nd home-work	3rd test	Project - Scope	Project - method-ology	Project - Model
5	10	5	10	10	5	5	10

Project - Results	Project - Discuss-ion	Project - Report Quality	Project - Present	4th test / exam	4th home-work	TOTALS
5	5	5	5	15	5	100