Help Wanted: Military Rotorcraft System Safety Engineering Academic Program Designers!

Steven Hosner, QinetiQ North America, PE
BS MSU (Michigan State University)
BS FVSC (Fort Valley State University)
MS MU (Mercer University)
BBB SOHK (School of Hard Knocks)

Courses of study

- The following slides will include MS and PhD system safety engineering courses of study for complex, highly integrated electrical, electronic and software systems
- Your mission, Mr. Phelps, should you choose to accept it, is to point out what is right or wrong with the courses and what needs to be done to fix it.

ASSUMPTIONS AFFECTING COURSE SELECTIONS

- The degrees are for electrical, electronic or software engineers working in military rotorcraft system safety engineering
- Most of the functionality of rotorcraft electrical and electronic systems will be implemented in software
- Rotorcraft electrical and electronic systems will tend to be complex and highly integrated systems

ASSUMPTIONS AFFECTING COURSE SELECTIONS (CONTINUED)

- Military rotorcraft must be qualified for unrestricted operation in civilian airspace in Instrument Meteorological Conditions (IMC) and operations under civil Instrument Flight Rules (IFR)
- Military rotorcraft must be qualified for unrestricted operation in military airspace in Instrument Meteorological Conditions (IMC) under Instrument Flight Rules (IFR)
- Question: Is there a difference between civil and military Instrument Flight Rules?

ASSUMPTIONS AFFECTING COURSE SELECTIONS (CONTINUED)

- Safety requirements, for a given hazard severity, are:
  - **Hazard probability of occurrence**
    - For civil functions, defined by the FAA
    - For military functions, must be acceptable to program management
  - **Development assurance requirements** applied to mitigate the possibility of design errors
  - Civilian hazard probability of occurrence is more stringent than military
  - Civil and military development assurance requirements are fast approaching concensus

ASSUMPTIONS AFFECTING COURSE SELECTIONS (CONTINUED)

- System safety engineering must provide safety requirements in a timely manner to influence design, development and qualification (A tip o' the hat to Mr. Steve Mattern!)
- System safety engineering starts when the project is started and little to no information about the implementation will be known and continues throughout the project to influence design, development and qualification

ASSUMPTIONS AFFECTING COURSE SELECTIONS (CONTINUED)

- System safety engineer will need to use concepts and techniques that:
  - Will be equally convincing to both civil authorities and military program managers
  - Are top-down from a very high level of functional abstraction down to wires, resistors, etc.
- Focus is on qualifying the ‘basic truck’ of the rotorcraft (Thank you Mr. Garry Mercaldi!), not on qualification of the myriad types of equipment required for airspace entry

MS COURSE OF STUDY OVERVIEW

- MS Course of study:
  - First Minor - 6 credits in statistics and reliability prediction
  - Second Minor - 6 credits in process and analysis
  - 12 credits of ‘Core’ courses
  - 6 credits for thesis
  - 30 credits total
- Typical for an MS degree
- 9 credits from Industrial Engineering, 6 from Computer Science, 3 from Mechanical and Aerospace Engineering and 6 from System Safety (new classes) + 6 credits thesis

MS FIRST MINOR – STATISTICS AND RELIABILITY PREDICTIONS

- Mark Twain "**Lies, damned lies, and statistics**“
- Statistics are the basis for reliability predictions
- Reliability predictions are the inverse of probability of failure which comes later
- Probability of failure is one of the key qualification requirements system safety must deal with
- My personal ignorance of this area is abysmal and it has cost me dearly in terms of credibility and self-esteem

MS FIRST MINOR – PROBABILITIES AND STATISTICS

Dept	Number	Title	Credits	Description	Preqs
ISE	690	Statistical Methods for Engineers	3	Application of statistics for estimation and inference using parametric and nonparametric methods. Descriptive statistics, sampling distributions, point and interval estimates, tests of hypotheses, ANOVA, and linear regression.	ISE 390 or permission of instructor
ISE	638	Engineering Reliability	3	Methodology of reliability prediction including application of discrete and continuous distribution models. Reliability estimation, reliability logic diagrams, life testing, and reliability demonstrations.	ISE 690

MS SECOND MINOR – PROCESS AND ANALYSIS

- Software process course:
  - Process is normally the way that development assurance requirements are implemented and substantiated
  - Understanding the basics of a good software development process is fundamental to understanding software development assurance requirements
  - Understanding the basics of a good software process makes the understanding of a good hardware development process much easier

MS SECOND MINOR – PROCESS AND ANALYSIS

- Object oriented analysis (OOA) and design (OOD) course
  - Analysis of complex, highly integrated systems is most amenable to analysis techniques used in OOA and OOD (abstraction, information hiding, etc.)
  - This course will be used as a basis to expand the use of abstraction, information hiding, etc. to analysis of system functions that are not strictly software for FHAs, PSSAs

MS SECOND MINOR – PROCESS AND ANALYSIS

Dept	Number	Title	Credits	Description	Prerequisites
CS	650	The Software Engineering Process	3	The process of developing complex software products. Includes software life cycles, phases of development and disciplines such as CM, QA, V&V, and T&E. Covers issues associated with professionalism and the ethical use of computers in the information age, including software piracy and copyrighting software.	CS 317, CS 490 and CS 424 or 524, or approval of instructor
CS	652	Object-Oriented Analysis and Design	3	A survey of formal and informal techniques and methodologies for software analysis, requirements, architecture and design. Emphasis is on effective development processes. Comparison of different approaches, considering their advantages and disadvantages.	CS 650 or approval of instructor.

MS CORE COURSES

- Human Factors Psychology – How effectively does the human interact with the system (Another area I am abysmally ignorant of!)
- System Safety – Analyses and programmatics for system safety per NASA and the military
- Governmental Aviation System Safety Requirements I – How to extract system safety requirements from government documents such as FAA regulations and guidance, MIL-STD-882, etc.

MS CORE COURSES

- Functional Hazard Assessment, Preliminary System Safety Assessment
  - Recognized methods by which functional hazards are defined and functional hazard safety requirements are set
  - Implements the top-down functional analysis/requirements process
  - Builds on the analysis techniques covered in the OOA and OOD course

CORE COURSES

Dept	Number	Title	Credits	Description	Prereqs
ISE	503	Human Factors Psychology	3	Study of human performance in human-technology-environment systems. Consideration of human capabilities and limitations as related to controls and displays, and the role of human cognition in decision-making and training effectiveness.	Graduate standing
MAE	639	System Safety	3	The process of system safety from the creation and management of a safety program on a system under development to the analysis that must be performed as this system is designed and produced to assure acceptable risk in its operation. Full discussion of the management and analysis processes and procedures. Incorporates the safety procedures used by the Department of Defense and NASA. Basic statistical methods and network analysis methods which provide an understanding of the engineering analysis methods are covered.	ISE 638
SS	100	Govtal Aviation Sys Sfty Reqts I	3	Developing system and safety requirements based on military and civil governmental regulations and guidance for safety critical systems.	Graduate standing
SS	120	FHA, PSSA	3	FHA and PSSA Setting Design Requirements for Safety Critical Aviation Systems; Use of ARP4761, ARP4754 and fault trees to substantiate system/software component relationships and allocate qualitative and quantitative safety requirements	CS 650, CS652

PhD COURSE OF STUDY OVERVIEW

- PhD Course of study:
  - 15 credits of ‘Core’ course
  - First Minor - 9 credits in statistics and reliability prediction
  - Second Minor – 9 credits in modeling, analysis and formal methods
  - Third Minor - 6 credits software testing
  - Fourth Minor – 6 credits in human factors

PhD COURSE OF STUDY OVERVIEW

- PhD Course of study:
  - Fifth Minor – 6 credits in process and development assurance
  - Core – 12 credits of ‘core’
  - Dissertation - 18 credits
  - 69 credits total
- 15 credits from Industrial Engineering, 15 from Computer Science, 3 from Mechanical and Aerospace Engineering and 18 (new classes) from System Safety +18 credits dissertation

PhD COURSE OF STUDY OVERVIEW

- Usually it is 24 credits major, 12 credits first minor, 12 credits second minor and 18 credits dissertation
- This interdisciplinary course of study has 5 minors, core classes and dissertation
- Could declare some of the ‘minor’ classes ‘core’ classes, but need advice from academic types on that

First Minor – Statistics, Reliability Prediction and RAM

- Statistics and Reliability Prediction the same as for MS degree
- Reliability, Availability and Maintainability
  - Includes MIL-HDBK-217 analysis which can be used for logistics purposes as well as conservative values for probability of failure
  - Traditionally, military safety program overlaps some with the RAM program since the military has included $ cost due to failure due to unique perspective of military as developer, integrator, owner, operator and maintainer of system

First Minor – Statistics, Reliability Prediction and RAM

Dept	Number	Title	Credits	Description	Prereqs
ISE	638	Engineering Reliability	3	Methodology of reliability prediction including application of discrete and continuous distribution models. Reliability estimation, reliability logic diagrams, life testing, and reliability demonstrations.	ISE 690
ISE	690	Statistical Methods for Engineers	3	Application of statistics for estimation and inference using parametric and nonparametric methods. Descriptive statistics, sampling distributions, point and interval estimates, tests of hypotheses, ANOVA, and linear regression.	Approval of instructor
ISE	738	RAM	3	In-depth application of decision theory and MIL-HDBK-217, and maintenance engineering techniques in order to achieve targeted reliability, availability and maintainability design goals.	ISE 638

Second Minor – Analysis, Modeling and Formal Methods

- Analysis the same as for MS degree
- Modeling is an expansion of analysis looking at different methodologies
- Formal Methods:
  - An introduction to mathematical basis for modeling and specifications of systems and/or software
  - Provides a rigorous method of specifying systems
  - Gaining more acceptance as viable for purposes of reducing V&V requirements

Second Minor – Analysis, Modeling and Formal Methods

Dept	Nmbr	Title	Crdts	Description	Prereqs
CS	551	Software Modeling	3	A survey of techniques and methodologies for software modeling. General modeling (e.g., UML), formal models, model checking, limitations of modeling, validation of models, domain modeling, model-driven architecture. Comparison of different approaches, considering their advantages and disadvantages.	Approval of instructor
CS	652	Object-Oriented Analysis and Design	3	A survey of formal and informal techniques and methodologies for software analysis, requirements, architecture and design. Emphasis is on effective development processes. Comparison of different approaches, considering their advantages and disadvantages.	CS 650 or approval of instructor
CS	655	Formal Methods in Software Engineering	3	Formal mechanisms to specify, validate, and verify software systems. Propositional and predicate calculi. Program verification through Djikstra's weakest preconditions and Hoare's method. Formal specification via algebraic specifications and abstract model specifications.	CS 650 and approval of instructor

Third Minor – Software Testing

- Covers a key element of development assurance requirements, software testing
- Software Testing – software testing techniques
- Software Test Coverage Analysis – Determines the coverage achieved with the testing

Third Minor – Software Testing

Dept	Nmbr	Title	Crdts	Description	Prereqs
CS	656	Software Testing	3	Advanced software testing techniques, including white box, black box, integration testing, and system testing. Other topics may include test data adequacy, test data selection, and output oracle, including functional, structural, and fault-based testing methods.	CS 650
SS	6	Software Coverage Testing Analysis	3	Analysis of software testing to determine achieved software coverages	CS 656

Fourth Minor – Human Factors

- Humans form a key part of rotorcraft systems
- Human Factors Psychology – How effectively does the human interact with the system – Same as for the MS degree
- Designing systems better for human use

Fourth Minor – Human Factors

Dept	Nmbr	Title	Crdts	Description	Prereqs
ISE	503	Human Factors Psychology	3	Study of human performance in human-technology-environment systems. Consideration of human capabilities and limitations as related to controls and displays, and the role of human cognition in decision-making and training effectiveness.	Graduate standing
ISE	624	Human Factors in Systems Design	3	Psychological, physiological, and anthropometric requirements for human beings and the integration of these requirements into the design of tools, machines, and systems.	Graduate standing

Fifth Minor – Process and Development Assurance

- Humans form a key part of rotorcraft systems
- Human Factors Psychology – How effectively does the human interact with the system – Same as for the MS degree
- Designing systems better for human use

Fifth Minor – Process and Development Assurance

Dept	Nmbr	Title	Crdts	Description	Prereqs
CS	650	The Software Engineering Process	3	The process of developing complex software products. Includes software life cycles, phases of development and disciplines such as CM, QA, V&V, and T&E. Covers issues associated with professionalism and the ethical use of computers in the information age, including software piracy and copyrighting software.	Approval of instructor
SS	130	Airworthiness Development Assurance Requirements	3	Application of development assurance requirements to ensure airworthiness. Includes application of DO-178, DO-254, MIL-STD-882 and other military requirements/guidance.	CS 650

Core – Process and Development Assurance

- Governmental Aviation System Safety Requirements I & II – How to extract system safety requirements from government documents such as FAA regulations and guidance, MIL-STD-882, etc.
- System Safety – Analyses and programmatics for system safety per NASA and the military (Same as for MS program)
- Use of ARP4754 safety assessment process and ARP4761 safety assessments

Core – Process and Development Assurance

Dept	Nmbr	Title	Crdts	Description	Prereqs
SS	100	Gvrnmntl Avtn Sys Sfty Rqts I	3	Developing system and safety requirements based on military and civil governmental regulations and guidance for safety critical systems.	Graduate Standing
SS	110	Gvrnmntl Avtn Sys Sfty Rqts II	3	Developing system and safety requirements based on military and civil governmental regulations and guidance for safety critical systems.	Graduate Standing

Core – Process and Development Assurance

Dept	Nmbr	Title	Crdts	Description	Prereqs
MAE	639	System Safety	3	The process of system safety from the creation and management of a safety program on a system under development to the analysis that must be performed as this system is designed and produced to assure acceptable risk in its operation. Full discussion of the management and analysis processes and procedures. Incorporates the safety procedures used by the Department of Defense and NASA. Basic statistical methods and network analysis methods which provide an understanding of the engineering analysis methods are covered.	ISE 638 Open to graduate students only.
SS	120	FHA, PSSA, SSA	3	FHA and PSSA Setting Design Requirements for Safety Critical Aviation Systems; Use of ARP4761, ARP4754 and fault trees to substantiate system/software component relationships and allocate qualitative and quantitative safety requirements	None

Thhaattts all folks!

- Suggestions?