Outline

- Welcome
- Software in Safety Critical Systems "Club"
- Introduction to MIT Aero/Astro Department plans
- Software Engineering Research Lab (SERL)

Software in Safety Critical Systems Club

- Impetus for this meeting
- Goals for a "club"
- Possible Activities
  - Information Sharing
  - Technology Transfer (tutorials, etc.)
  - Tool Fairs
  - ????

The MIT AA Dept. Strategic Plan

A department focused on the vibrant, but redefined, field of aerospace:

Vehicle Engineering (Propulsion and Airframe)

Structures, Materials, Fluids

Information Engineering

Software Engineering
Human-Computer Interaction
Autonomy
Communications

Systems Architecture and Engineering

Department Activities in Information Technology

- Education
  - New undergraduate major

    Bachelor of Science in Aerospace Engineering with Information Technology
  - M.Eng., M.S., and Ph.D. programs
  - Industry internships
- Research

AA Dept. Research in Information Technology

Software Engineering Research Lab (SERL)

Nancy Leveson

- Engineering for Safety
- Model-Based System and Software Engineering
- Requirements Specification and Analysis
- Human-Centered Automation

International Center for Air Transportation (ICAT)

John Hansman, James Kuchar, Eric Feron

- ATC Modernization
- Aircraft Automation (FMS)
- Alerting Systems
- Complexity Measures
- Unmanned Air Vehicles (UAVs)

Space Communications and Networks

Eytan Modiano, Vincent Chan

- Protocols for Hybrid Networks
- Satellite Network Architecture
- Communication for Air Vehicles
- Mobile Ad Hoc Networks

Space Systems Lab (SSL)

Brian Williams, David Miller

- Distributed Satellite Systems
- Model-Based Autonomous Systems
- Automated Reasoning and Artificial Intelligence
- Cognitive Robotics

Software Engineering Research Laboratory

Graduate Students

John Bellingham
Mirna Daouk
Danny Lai
Pong Lee
William Melendez
Israel Navarro
Natasha Neogi
Jayakanth Srinivasan
Sean Sutherland
Maxime de Villepin
Marc Zimmerman

Undergraduate Students

Emily Craparo

Postdocs

Ed Bachelder (MIT)
Kristina Lundqvist (Uppsala Univ.)

Visitor

Masafumi Katahira (NASDA)

Goals:

- Advance the state of the art in system and software engineering of safety-critical systems
- Promote information interchange

Activities:

- Fundamental Research
- State of the art projects with government and industry
- Workshops, short classes, extended visits, interchanges
- Tech transfer and commercialization

Software Engineering Research Laboratory

Progress since started in 1999:

- Nine master's theses completed
- Funding from NASA, NSF, Air Force, Raytheon, Draper Lab
- Joint projects:
  - Air Traffic Control: Eurocontrol, Raytheon
  - Autonomous Vehicles (helicopters): Draper
  - Reducing Cycle Time for Operational Upgrades:
    AF Air Combat Command
- Open positions for faculty (Ph.D.) and staff researchers (M.S.)
- Three new classes in software engineering (more will be developed as more faculty are hired)

New Classes in Software Engineering and System Safety

16.35 Aerospace Software Engineering

Concepts, methods, and tools for the specification, design, construction, verification (testing and analysis), and documentation of large software systems, particularly real-time embedded software. Includes project management fundamentals essential to creating complex software systems successfully. Students work together on a large team project following the process required for FAA certification of airborne systems (DO-178B).

16.355 Advanced Software Engineering

Learning to exercise professional judgement in selecting an approach for a particular project based on an understanding of how the present state of software engineering practice came about, what was tried in the past, what worked and what did not, and why. Specific topics covered: process and lifecycle; requirements and specifications; design principles; testing, formal analysis, and informal reviews; quality management and assessment; metrics, COTS, and reuse; team organization and people management; software engineering aspect of programming languages.

16.358 System and Software Safety

Concepts and techniques for building high-integrity or safety-critical systems that have software components. Topics inclucd the nature of risk, formal accident and human error models, fundamental concepts of system safety engineering, system and software hazard analysis, designing for safety, fault tolerance, safety issues in the design of human-machine interaction, verification of safety, and management of safety-critical projects. Includes a class project involving the design and analysis of a safety-critical system.

SERL Research Topics

Model-Based System Engineering

- Modeling and executable specification languages
- Analysis techniques and tools
- Animation of models (visualization)

Projects include:

Air Traffic Control

MD-11 Flight Management System

NASA Robot

Autonomous Helicopter

Status:

Fundamental research and evaluation
Starting commercialization of tools

Engineering for Safety

- Methodology for building safety-critical systems that include software and complex human decision making.
- New hazard analysis techniques
- Integration of safety information into system development tools
- New accident models

Projects include:

Air Traffic Control
NASA Tesselator Robot
Analysis of recent aerospace accidents

Status:

Fundamental research and evaluation on real systems
Technology transfer through industry classes

SERL Research Topics (cont.)

System and Software Specification

- Structuring methods to enhance problem solving ability, traceability, and capturing of design rationale
- Completeness of requirements specification
- Reviewability and readability

Projects include:

Air Traffic Control
NASA Robot
TCAS II
Various aerospace systems

Status:

Fundamental research and evaluation
Starting commercialization of first tools

Human-Computer Interaction

- Task analysis and allocation
- Reducing mode confusion and other human errors
- Enhancing learnability
- Tailoring automation design to operator requirements (human-centered design)

Projects include:

Air Traffic Control

NASA Robot

Status:

Fundamental research and evaluation

SERL Research Topics (cont.)

Software Evolution

- Specification and design to reduce impact of requirements changes
- Reducing costs of re-evaluation of safety

Status:

In initial stages

Software Assurance

- Test data generation from specifications and behavioral models
- Requirements coverage analysis

Status:

In initial stages