CIS 890: High-Assurance Systems

Spring 2024

Lecture 0: Course Administration

CIS 890 People

- Instructors
  - John Hatcliff (hatcliff@ksu.edu)
- Helpers
  - Jason Belt (PhD student working in the SAnToS Research Group)
  - Brian Larson (formal associate of SAnToS Lab with decades of experience in safety-critical systems)

Course Web-site

- The URL for the course web-site is…
  - http://highassurance.santoslab.org
- The Syllabus link provides the official policies of the course
- The Course Schedule link provides the schedule of lectures, quizzes, assignments, and exams for the course. You will need to monitor this page closely.
- The Lectures links provides links to all the content artifacts (video, slides, examples, etc.) for the course.
- We may also make use of the K-State Online web-based infrastructure as explained on the following slide…

Course Resources

- Course web-site
- Papers to read
- Online lectures
- Software development tools
- Homework assignments
- Course project resources

Course Strategy

Course lectures will illustrate concepts in end-to-end development of safety-critical systems using a simple temperature controller example

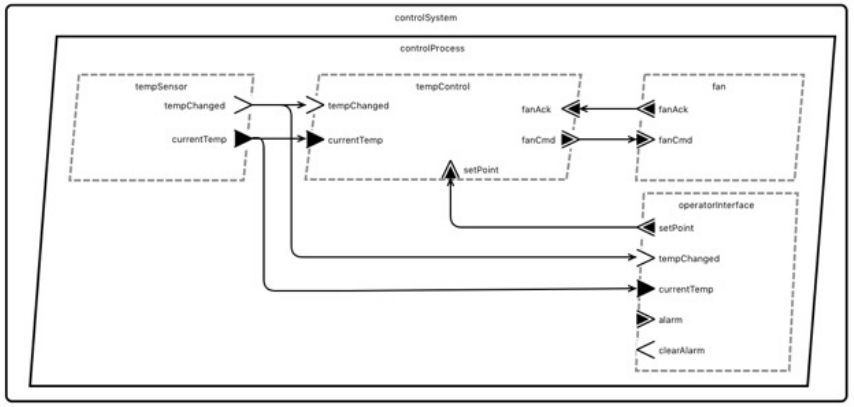
- Architectural models in AADL and SysMLv2
- Implementations in HAMR/Slang
- Formal specifications, property-based testing, Logika verification
- User Interfaces (collaboration - Cat Liang)
- Interfacing to sensors and actuators (collaboration - Jacob Legg)

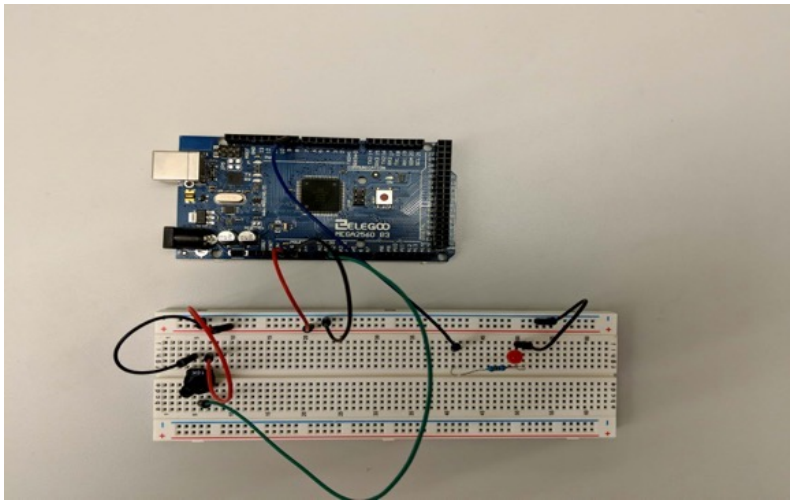
Course project will involve students contributing to different aspects of the development of materials for several more realistic systems

- PCA Pump (medical device)
- Isolette (medical device)
- …other aspects of interest to students

Temperature Control - Lecture Example

- Simple safety critical system used to illustrate many concepts in this course
- Used as ”hello world” example in SAnToS research on building control
- Simple version of Isolette example
- We will illustrate end-to-end development
  - Models, Slang code, C code, running on STM32/Arduino boards, with hardware





Possible Projects

- PCA Pump
  - Open source medical device developed as part of a US Department of Homeland Security project
  - Emphasis
    - cleaning up requirements
    - Refactoring architecture to make it more amenable to GUMBO contracts, testing, verification
    - Refactoring existing implementation, adding verification, testing
    - Preparing artifacts for public release
- Isolette
  - Small medical device example
  - Emphasis is on polishing artifacts for public release
- Students should be able to tailor projects to their interests

PCA Pump – Course Project

Patient-Controlled Analgesic Pump

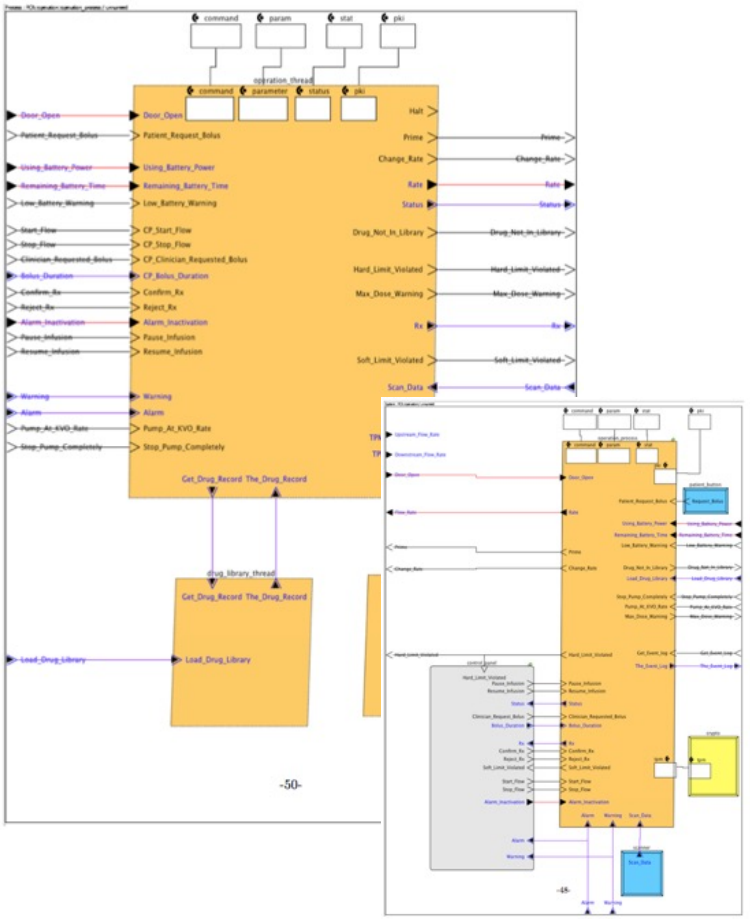
- Patients are commonly given patient-controlled analgesics after surgery
- Crucial to care, but numerous issues related to safety

http://patientsafetyauthority.org/PATIENTSCONSUMERS/PatientConsumerTips/Pages/PCA_Pump_Consumer_Tips.aspx

PCA Pump Artifacts

KSU is developing a collection of artifacts (over 8+ years), previously in consultation with FDA engineers and Galois engineers

- 100+ page requirements document written following FAA Requirements Engineering and Management Handbook
- Architecture formally defined in AADL
  - Adopts a safety architecture approach
- Slang implementation
- GUMBO artifacts and associated testing / verification
- Alternate
  - Behavioral interface specification in BLESS
  - Internal behavior and proofs of correctness in BLESS
- Associated hazard, risk management, and regulatory artifacts (leveraging the AADL Error Model Annex)
  - One focus is formal definition and risk assessment associated with ICE interface
- [optional] UI framework
- [optional] Prototype hardware platform for classroom and research use



ISOSCELES Project

- Joint KSU/Adventium Labs Project
- Funded by Department of Homeland Security
- Goals
  - develop an open source reusable platform for medical device development
  - use the platform to build a PCA pump
  - Illustrate best practices in rigorous development
- The lectures and project material in this course are feeding into the ISOSCELES project

Isolette

The example system that we will consider is an "isolette" – an infant incubator used to warm and monitor new born babies

http://www.karencheng.com.au/category/pregnancy/page/2/

Our inspiration to use the Isolette comes from its presentation in the FAA DOT/FAA/AR-08/32, *Requirements Engineering Management Handbook* by David L. Lempia & Steven P. Miller.

Homework Assignments

- Individual assignments will include…
  - Quizzes
  - Contributing to requirements writing and other development artifacts
- Project
  - Each student will contribute something to a set of development artifacts associated with a your assignment team project

- Good luck in the course, and we hope you enjoy it!