EECS 159A Project Report

Due December 6, 2019

Each team should submit a project report (one report per team). This report should follow traditional formatting for scientific and engineering papers. The IEEE transactions (journal paper) template should be used, found here:

https://journals.ieeeauthorcenter.ieee.org/create-your-ieee-journal-article/authoring-tools-and-templates/ieee-article-templates/templates-for-transactions/

The instructions in the above link are comprehensive, but in general, your report will include these features:

Your Impressive Academic-Sounding Title
Team Member Names plus your
Project Advisor's Name.

Abstract: One paragraph summarizing the goals, methods and results of your work. Don't just say what you are *going* to talk about in the body, but instead actually state the results, etc., in a brief but fully self-contained way.

Introduction: One to three paragraphs introducing the project and its goals, background discussion of prior approaches and results, and some overview discussion of your methods and results.

The **main body** of the work is typically subdivided into chapters or sections that are likely individual to your own work. For example, if your work involves both hardware and software, you will likely want to include chapter titles and possibly sub-titles (breaking things down further) for each of these topics. A few additional common sub-divisions include discussions of equipment and materials, methods, simulation results, prototype results and performance, etc. Figures, tables, photos, etc., should be included whenever they are useful.

Summary and Conclusions: One to three paragraphs summarize the results *without* duplicating text from the abstract, etc. Note that "conclusions" are distinctly different from a "summary" of the work.

Acknowledgements: In this section, provide a brief acknowledgement of those who helped you in some way – your advisor, the funding sources you received, loans of equipment that you benefitted from, etc.

References: A minimum of four references should be provided, e.g. selected from the fundamental papers in the field and/or those that especially helped inform your work. These should be in IEEE format. Note that references should not merely be listed in isolation, they should be *actually referenced* in the body of the paper.

Appendix: Due to the ABET reviewer's comments, you are asked to include responses to these specific issues in an appendix:

1) What **technical standards** were relevant to your projects, how did you pick between them, and was your resulting design compliant with these standards? Some simple ones include Bluetooth version, WiFi version, USB version, SD card type, etc., but many more specialized standards exist too. Non-compliance can easily occur if, for example, FAA, FCC, etc., regulations are ignored, off-spec or counterfeit parts are used, and so on. Please review the standards document available on the class web site and as discussed in class.

2) What **constraints** have you faced in designing and building your projects and how did you cope with them? Examples of possible constraints include accessibility issues, safety code issues, constructability, cost (always a big one), power constraints, ergonomic difficulties, constraints that affect the ability to extend the functionality and interoperability of the project, legal considerations, maintainability issues, manufacturability, marketability, policy and regulatory issues, scheduling issues, sustainability issues, usability issues, etc. What constraints were important in your project and how did you work around them or solves them?

3) In our current world of unrelenting hacking and hidden vulnerabilities, what **hardware and software security issues** risked being present in your work and how did you mitigate them? What hardware insecurities did you face? For example, the "spectre" and "meltdown" problems are hardware insecurities that have plagued Intel over the last several years. Many, many software insecurities also exist, seemingly turning up at an exponential rate. What did you do identify security issues, which were found to be a threat, and what did you do to help prevent exposure to these vulnerabilities, etc?