

Cryptographic Design Project

Einar J. Aas, Bjørn B. Larsen, and Elena Hammari

Dept. of Electronics and Telecommunications, Norwegian University of Science and Technology, NORWAY

<Einar.j.aas|Bjorn.b.larsen|Elena.hammari>@iet.ntnu.no

ABSTRACT

The course *Realization and Test of Digital Components* is offered to 4th year's Master students. The course has gradually evolved to more student active methods. Portfolio assessment is integrated in the course. The portfolio is built from lab work, project work, and individual written exam. The students work in groups of two. Peer reviews are exploited to train the students in evaluation, and in being evaluated.

1. INTRODUCTION

The course *Realization and Test of Digital Components* has been offered to 4th year's Master students for several years. The course has evolved to more student active methods. Portfolio assessment is integrated in the course. Final course evaluation is done with different weights.

One important element of new engineering education programmes is more systematic use of Project Based Learning (PBL). We are convinced that *electronic engineering education* (EEE) lends itself very well to PBL because electronic design projects normally are integrated in EEE. The major challenge is the *designing of* design projects such that stated *learning objectives* are fulfilled.

One significant goal is to educate students in design competence. Specifically, we want our students to develop personal design competence, including specification, design tradeoffs, design for testability, synthesis, analysis and verification, and realization. Skilled use of commercially available CAD tools shall be ingrained in the design competence. We have employed PBL methodology extensively in the past, and gained much experience on how it can be applied successfully [1 – 6]. Metrics for design quality and design efficiency were developed to measure designs, see e.g. [5].

Other engineering institutions have also employed PBL and concurrent engineering principles in design classes. For example, in [7], collaboration with regional industry, while introducing 'design to cost' methods, proved to be very stimulating for the students.

2. PROJECT ORGANIZATION AND DELIVERABLES

The class is partitioned into groups of two persons each. Each group works together with three laboratory tasks and one large design project. In addition, peer review reports are developed, and one oral presentation is given. In order to train evaluation skills, each student is grading the oral presentations of all other groups.

Deliverables during the course include: Architecture Design report, Detailed Design report, proof of decryption of given RSA-encrypted message, and three Laboratory reports. A detailed time schedule is given, deploying important dates and deliverables, see Tab. 1.

3. PEER REVIEW PROCESS

Twice during the project period, every group is evaluated by another group. The main goal of peer evaluations is to train the students in judging other professional's work.

Table 1 Time schedule and deliverables

week	tasks
34	Intro to RSA crypto. Read <code>intro_doc</code> .
36	Spec given. Read.
38	Deliverable_1 introduced. Detailed <i>Content</i> listed. Evaluation criteria included. Template for individual time recording given. Deadline given. This deliverable to be peer reviewed.
39	Make structure for Deliverable_1 . Peers shall be able to comprehend <i>what and why</i> .
41	<date>: turn in Deliverable_1 , and send to peers. Read peer_evaluation-template_1 . Evaluate, and submit. Plan meeting with peers for mutual oral evaluation.
42	<date>: deadline for return of peer_evaluation_1 . Start to read, reflect, and write how you judge the evaluation of you.
43	<date>: deadline for your comments to the evaluation. What did you learn?
44	Start detailed design! Develop comprehensive verification plan. Start writing Deliverable_2 .
45	<date>: turn in Deliverable_2 . Procedure as for Deliverable_1 .
46	<date>: peer_evaluation_2 .
47	<date>: turn in final report. Oral presentation from each group.

We emphasize concrete and constructive comments, including exposure of design flaws, oversights, ambiguities, efficiency and quality of the designs, contradictions or incomplete descriptions. In addition, the students shall give marks (A – F) on specific aspects of their peers' reports.

Two web-based templates are used to fill in and collect the evaluation. The first focuses on problem definition and architecture exploration. The tasks to evaluate are mentioned briefly in Tab. 2. The second evaluation focuses on the VHDL code, and the comprehensiveness of verification.

Table 2 Evaluation tasks; first peer evaluation

No.	task
1	Readability, structure, completeness, block level doc, I/O signal doc, walk-through description
2	Problem description - completeness
3	Discussion of 2-3 feasible concepts, selected concept, analysis of area and performance
4	Verification, autonomous test bench, comprehensive verification?
5	What did you learn from your peers?
6	Total impression
7	Comments to this evaluation process

Most comments offered were concrete, with suggestions for improvements, revelation of design flaws, and demands for more thorough documentation. "*Incomplete*

