ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

REVIEWER'S OPINION OF FINAL THESIS

I. IDENTIFICATION DATA

Thesis name:	**Industrial Control System Security Analytics**
Author's name:	**Marcel Nemet**
Type of thesis :	master
Faculty/Institute:	Faculty of Electrical Engineering (FEE)
Department:	Department of Computer Science and Engineering
Thesis reviewer:	PhD Sebastian Garcia
Reviewer's department:	Department of Computer Science and Engineering

II. EVALUATION OF INDIVIDUAL CRITERIA

Assignment **ordinarily challenging**

Evaluation of thesis difficulty of assignment.

The thesis has the standard difficulty for a development master thesis.

Satisfaction of assignment **fulfilled with minor objections**

Assess that handed thesis meets assignment. Present points of assignment that fell short or were extended. Try to assess importance, impact or cause of each shortcoming.

The thesis meets the required assignments. The points where the thesis fell short are:

- The focus of the written thesis should have been more on the development and design and less in the description of the algorithms.
- The evaluation of the development was not done thoroughly. This means that the design and draft versions were not evaluated by the users during the development and therefore the feedback of the users was not incorporated early in the code.

The importance of the thesis is high. IBM and most companies dealing with data have an urgent need to help their analysts better analyze the data with semi automated tools. This type of tools can make a huge difference.
The impact of the thesis is probably moderate because to be successful the system will need to be maintained in IBM, which is more difficult without the student there. Also the impact for the University is low because the code is not available and the experience does not help other researchers.

Method of conception **correct**

Assess that student has chosen correct approach or solution methods.

The student has chosen the correct solution method by designing the system accordingly to the needs of IBM. He developed it to fulfill those needs, including a final evaluation of the system with interviews.

Technical level **C - good.**

Assess level of thesis specialty, use of knowledge gained by study and by expert literature, use of sources and data gained by experience.

The technical level of the thesis is good, and the student used the knowledge gained during his university studies to solve the thesis problem. His use of the data provided by IBM was satisfactory.

Formal and language level, scope of thesis **B - very good.**

Assess correctness of usage of formal notation. Assess typographical and language arrangement of thesis.

Whenever needed, the formal notations and diagrams where used correctly. Also the thesis is well explained.

Selection of sources, citation correctness **E - sufficient.**

Present your opinion to student's activity when obtaining and using study materials for thesis creation. Characterize selection of sources. Assess that student used all relevant sources. Verify that all used elements are correctly distinguished from own results and thoughts. Assess that citation ethics has not been breached and that all bibliographic citations are complete and

in accordance with citation convention and standards.

This thesis could have beneficiated from a more thorough search of sources. The security problems of ICS systems were referenced, but not the previous works on systems to assists the analyst of ICS systems. Given that this thesis is about the development of a system to assist analysts, references of similar systems was in order.

Additional commentary and evaluation

Present your opinion to achieved primary goals of thesis, e.g. level of theoretical results, level and functionality of technical or software conception, publication performance, experimental dexterity etc.

The primary goal of the thesis was fulfilled: to develop a system that assists analysts in the evaluation of anomaly detection algorithms in ICS. The software seems to be completely functional and done with the quality required by IBM.

III. OVERALL EVALUATION, QUESTIONS FOR DEFENSE, CLASSIFICATION SUGGESTION

Summarize thesis aspects that swayed your final evaluation. Please present apt questions which student should answer during defense.

- Summary: The thesis made by Marcel dealt with a very complex problem: The assistance of human analysts while evaluating machine learning algorithms. This is a hard topic that needed both technical experience and skills in human-computer interaction. He created an interface for the analysts to evaluate the anomaly detection algorithms used in Industrial Control Systems (ICS), dealing with knowledge about the algorithms and evaluations from the analysts.
- Questions:
    - It seemed that the specific problem that you where trying to solve was not quite clear in the thesis. Can you clarify the problem?
    - What was the justification of using interviews as the evaluation process?
    - What is your conclusion about the final evaluation of your thesis by the users? Would you say that they are completely satisfied and they are going to use it? If not, elaborate quickly why.
    - What are the two more important things that you learned doing your thesis?
    - What is your analysis on the bias introduced by the users identifying what an anomaly is and then selecting the testing data and parameters of the algorithms to try? Do you think that the results may be skewed?
    - Which would you say would have been a more analytical way of evaluating the final system?
    - The work done seems to have been very hard and time consuming, however this was not appropriately reflected in the written thesis. Why do you think this happened?
    -

I evaluate handed thesis with classification grade**C - good.**

Date: **19.1.2017** Signature: