**241b Advanced Computing for Chemical Plant Security Assessment**

*Cristina Piluso, Korkut Uygun, and Yinlun Huang*

Homeland security, and more specifically chemical plant security, is one of the most critical tasks in the nation today. The tragedies of September 11, 2001, have profoundly affected our nation on multiple fronts. Chemical facilities, where toxic or hazardous chemicals are manufactured and housed, present an attractive target for terrorists, intent on causing massive damage. Given the fact that chemical processes are often operated under high temperatures and pressures, fast material, energy, and momentum flows, and complex reaction and separation mechanisms, results in the fact that chemical processes are typically risky and more environmentally detrimental than other manufacturing industries. The impact and massive damage of an attacked chemical plant on the environment, economy, and society are potentially harmful and immeasurable. The threats of terrorism have greatly alerted the chemical process industries to assure plant security at all levels, including infrastructure improvement focused physical security, information protection focused cyber security, and design and operation improvement focused process security. The development of effective plant security methods and technologies is therefore of great and urgent interest for the chemical industry and beyond.

In this work, we introduce a novel modeling framework for security analysis and assessment of chemical processes. The core of the method introduced is a multiple intermediate modeling framework for fast and automatable dynamic simulation of chemical plants on a full scale. The basic idea is to utilize a rigorous simulation of a plant, which is accurate but requires human supervision, to generate process security relevant data for each process unit under various security threat scenarios. This data is used to train data-driven models, such as Artificial Neural Networks (ANN) models, to predict the dynamic responses of each sub-process/unit in the flowsheet. These individual, “intermediate” models are then interconnected to form a plant-wide security model that predicts all security-relevant information for the entire plant. There are three major advantages of this approach: (i) The simulation of the intermediate plant model cannot fail to converge (a common problem in most process simulation software), hence requires no human supervision; (ii) the simulation requires a drastically reduced amount of CPU time, and (iii) multiple models are ideal for parallel computing, and hence parallel computing and CPU clusters may be very efficiently utilized to ensure that the results of the security analysis, which requires a nonlinear optimization that has typical issues about the globality of the solutions, are reliable.

In this particular work, a dynamic simulation of a known Vinyl Acetate Monomer (VAM) production plant, using the HYSYS process simulation software, was developed for process security analysis. The modeling method outlined above was employed to create a practicable intermediate model for the VAM plant. This intermediate model was then used in a stochastic search algorithm in a 20 CPU cluster system to solve a nonlinear dynamic optimization problem and identify possible disaster scenarios for the process, and hence provide a model-based security assessment for the plant.