PROCESS SECURITY IN CHEMICAL ENGINEERING EDUCATION[†]

Cristina Piluso, Korkut Uygun, and Yinlun Huang[*]
Department of Chemical Engineering and Materials Science
Wayne State University, Detroit, MI 48202

Helen H. Lou
Department of Chemical Engineering
Lamar University, Beaumont, TX 77710

Original: April 9, 2004
Revision: September 23, 2004

Abstract

The threats of terrorism have greatly alerted the chemical process industries to assure plant security at all levels: infrastructure-improvement-focused physical security, information-protection-focused cyber security, and design-and-operation-improvement-focused process security. While developing effective plant security methods and technologies is urgent for the industries, identifying and integrating plant security elements into undergraduate curriculum is vital for a new generation of engineers. This paper discusses the necessity and explores opportunities of integrating Process Security concepts into undergraduate curriculum, mainly through Process Design and Process Safety courses. An educational tool to assist in this effort is also presented, along with a sample case study to be utilized in classroom teaching.

---

† For publication in *Chemical Engineering Education.*
* All correspondence should be addressed to Prof. Yinlun Huang (Phone: 313-577-3771; Fax: 313-577-3810; E-mail: yhuang@wayne.edu).

INTRODUCTION

The tragedy of September 11, 2001, and subsequent terrorist attacks have alerted greatly the chemical process industries for plant security assurance at all levels: infrastructure-improvement-focused Physical Security, information-protection-focused Cyber Security, and design-and-operation-improvement-focused Process Security. Process Security is possibly the most difficult task due to the level of sophistication involved in integrating security with the production process.

Security as a whole is an extremely complex subject due to its unpredictable and non-probable nature. Physical Security protects against attacks such as bombings, theft, or sabotage, by armed terrorists, disgruntled employees, political activists, and such[1]. Lemley *et al*.[1] discuss an approach to enhance the process hazard analysis (PHA) by including a relative risk assessment in order to establish physical security infrastructure and programs. In addition, they discuss physical security countermeasures, including communications with local law enforcement agencies, vehicle barriers to prevent driving through fencing, alarms, access control, security cameras, and double gate entries. Cyber Security is defined by Baybutt[2] as the protection of manufacturing and process control computer systems, along with their support systems, from adversaries interested in obtaining, corrupting, immobilizing, destroying, or prohibiting access to important information. Baybutt also describes asset-based methods for including cyber security vulnerabilities in the assessment of a Security Vulnerability Analysis (SVA). Examples of cyber resources include computers, servers, operating systems, e-mail, user names and passwords, process control data, and business plans, to name a few. Despite these countermeasures being outside the realm of typical chemical engineering practice, the significance of physical and cyber security should not be ignored.

It is recognized that traditional process safety measures alone are no longer sufficient for total plant security[3]. Process security is an extended concept and practice of process safety. However, while the typical scientific tools for safety assessment are based on probabilistic analysis, security incidents are intentional, rather than accidental. In the chemical process security arena, the major concern is the potential for an event resulting in a catastrophic outcome, such as explosions, toxic release, and loss of life[4]. If such an event is possible, even with a low probability, it has to be addressed and solutions must be found. Therefore, process security cannot take probability into account, as the adverse events by terrorists or saboteurs do not follow likelihood; they are completely unexpected. In this context, the attacks are referred to harmful manipulations by saboteurs who have sufficient technical knowledge, rather than to brute force ones that are in the scope of traditional security methods. Of course, no fundamental method can hope to prevent the consequences of a bomb being dropped on the facility. Still, developing better designed processes can reduce the inherent vulnerability of a process. Traditional process safety techniques that rely on steady-state information, likelihood, and preset alarm systems may not be sufficient for addressing process security problems.

With the first work describing Process Security, Lou *et al.*[3] suggested that process security should be a separate subject of interest, under a broader umbrella of safety methodologies, and the objective in process security studies should be the design of secure processes through use of rigorous and deterministic simulation-oriented methods. Note that while the objective is parallel with *inherent safety* studies[5], the suggested method of solution is quite different.

In this article, we discuss the value and necessity of the Process Security concept in undergraduate chemical engineering curriculum, as an addition to or extension of the existing process safety material. We will also introduce a process security analysis tool that is developed for educational use, which enables a seamless and easy integration of the process security concept to the process safety and process design materials.

PROCESS SAFETY AND SECURITY IN EDUCATION

It is well recognized that process safety is of primary importance to the chemical process industries and it is second nature for chemical engineers[6]. Thus, process safety should be systematically integrated into chemical engineering education. The Center for Chemical Process Safety (CCPS), under AIChE, has developed much information in the area of safety and disseminated it among industries and universities[7]-[9]. The Safety and Chemical Engineering Education (SACHE) Committee under CCPS has generated various educational products for undergraduate curricula for more than a decade[10]. These products have been used, at different levels of details and comprehensiveness, in a number of universities, including Texas A&M University, Wayne State University, and Michigan Technological University. Courses about process safety fundamentals and risk assessment are very popular in their chemical engineering programs at both the undergraduate and graduate levels[11]. Wayne State University has also developed several course modules and used in senior process design courses, under the grant from NSF's Course, Curriculum, and Laboratory Improvement (CCLI) Program. The process safety materials and the teaching experience accumulated by those universities should be valuable for other chemical engineering programs to integrate process safety into their curriculums.

Today, process safety education becomes more important than ever, especially due to the need of homeland security assurance. The nature of chemical industries, whether due to the toxicity and hazardousness of ingredients used, the highly exothermic nature of many reactions involved, or simply because of their importance as an essential component of the infrastructure, presents a possible security target. Naturally, the chief responsibility of handling these issues fall on the shoulders of chemical engineers who have the most insight into the process. As such, the concept of Process Security also becomes not just relevant, but also a critical element in chemical engineering education. Chemical engineers must be made aware of their responsibilities and roles with regard to process safety and security, and be educated about the existence of process security analysis methods and tools. This type of education is a long-term effort, but needs to be addressed immediately[12]. In chemical engineering, the available educational materials on process safety are truly valuable for this purpose. The concepts, scopes, and underlying principles and methodologies of process safety, however, should be extended to meet the need for process security[13],[14].

PROCESS SECURITY EVALUATION METHODOLOGY

The methodology used in this work is based on the Fast Security Assessment Theory introduced by Uygun *et al*.[15],[16]. Deterministic, model-based process security concept is a new subject with few related works[3]. An update of the instruction materials will be necessary as progress takes place in this area.

A security threat is defined as an incident that will result in disaster if no effective countermeasure is taken, typically occurring over a span of minutes or seconds[15]. Under this theory, a process is considered "secure" if the time needed to detect and eliminate the threat (denoted as Minimum Time to Disaster – MTD) is less than the time it takes for the system to move from a nominal operation to a disaster condition, assuming the worst conditions possible. It is quite apparent that these time limits are dependent on the reaction type and conditions present in the process in question. Uygun *et al.*[15],[16] have developed the following two fundamental definitions in process security studies.

Definition 1[16]. *In most chemical systems, a plant model consists of more than one system variable; yet only a few of these need to be used directly to define disaster boundaries, such as pressure. These variables are referred to as critical variables.*

Definition 2[15]. *A process is secure if:*

$$\tau \geq \tau^r \qquad (1)$$

where τ *(the Minimum Time to Disaster) is the minimum time required by the process to move from the nominal operation point to the disaster border;* τ^r *(the resolution time) is the minimum time needed for detecting the threat, making decisions, and taking necessary countermeasures to eliminate the threat. While an exact determination of the resolution time is difficult, a large value (e.g., > 15 minutes) for MTD is generally a mild vulnerability; beyond an hour should be considered secure, as this allows ample time to prevent a disaster.*

Accordingly, the process security problem is mathematically given as:

$$\tau = \min_{\mathbf{d}(t)} \int_0^{\tau} dt \tag{2}$$

s.t. $$\frac{d\boldsymbol{y}}{dt} = \boldsymbol{f}\left(\boldsymbol{y}, \boldsymbol{d}, \boldsymbol{p}\right) \tag{3}$$

$$y_c(\tau) = y_{c,d} \tag{4}$$

$$y_c(0) = y_{c,0} \tag{5}$$

$$\boldsymbol{d}^{min} \leq \boldsymbol{d}(t) \leq \boldsymbol{d}^{max} \tag{6}$$

where ***y*** is the vector of system variables; ***d***, the vector of disturbances. The reference points for defining the minimum time to disaster (τ) are the nominal operation point, $y_{c,0}$, and the disaster border, $y_{c,d}$, for the critical variable. Vector ***p*** is a constant vector of design parameters. Process security models (Equation 3) have various requirements different from normal process models. They should be able to describe the system to the limit of disaster. Also, it should be noted that in a security-threatening situation, both manipulated variables and disturbances may be the causes of security threat; hence they are both included as disturbances. Uygun *et al.*[16] further discuss that some state variables are also directly vulnerable to security threats and hence should be treated as disturbances as well.

γ -Analysis

The Process Security problem in equations (2-6) can be solved in various ways, including the calculus of variations and conventional numerical schemes employed for similar problems such as model predictive control. However, the convergence properties of existing dynamic optimization algorithms are generally poor if the models are nonlinear; this limits the reliability of the results. This problem is caused by the complexity introduced by time-dependence, which may cause the optimization algorithm to be trapped in local optima.

Uygun *et al*.[15] have devised a novel approach to simplify the solution process. The principal idea in the γ-analysis is to investigate the time-derivatives of the system dynamic equations directly. The method involves discretizing the differential equations along the critical variable to create a number of much simpler static optimization problems. This simplifies the problem significantly and reduces the complexity of the individual optimization problems drastically (as compared to conventional dynamic optimization schemes) so that the results are far more reliable, and can be obtained within seconds. The method generates a "confidence interval" where the MTD can fall in, rather than an estimate of the exact value. This allows a fast security assessment for the process either off-line or on-line; hence it is a justifiable engineering solution to the rather difficult problem of predicting how a saboteur's mind works.

In addition to providing a confidence interval for MTD, the γ-analysis method facilitates further process analysis, and hence a more thorough process security assessment. This assessment is performed through calculating the importance of each variable on the overall system security and the time to disaster; Uygun *et al*.[16] define the importance as each variable's "*significance*." Basically, this is a sensitivity analysis algorithm utilizing the γ-analysis method, and a calculated *significance* value is the relative change that would be observed in MTD if the particular variable were under control. A large significance value implies that the variable is critical for a disaster situation to occur. On the other hand, a value of zero significance suggests that the variable in question is not important from a process security point of view. Significance analysis is a key function for design/retrofit studies utilizing the γ-analysis method.

INTEGRATION OF PROCESS SECURITY INTO SENIOR DESIGN

The differences in the scope of the problem and implicit assumptions about the nature of the safety and security threats are already summarized in the preceding sections. However, another important difference is the methodology employed. Process safety is typically experience based, and employed through checklists and other managerial tools that may not be sufficiently adequate for integration into an engineering curriculum except specific safety courses. The vision in Process Security, however, is to construct first-principles-based deterministic models and utilize them (for instance with simulations) to gain knowledge about the vulnerabilities of the process, and if possible, to eliminate the vulnerabilities through modifying existing processes. As such, Process Security problems feature a combination of control, design, and modeling aspects, and thus require the students to be able to combine and apply the skills and information gained in core chemical engineering courses, such as mass and heat transfer, kinetics, unit operations, process control and design.

The major difficulty in integrating Process Security into undergraduate curriculum lies in this very multi-subject nature of the problem. It is only in the senior year of an undergraduate curriculum that the students can be expected to have a sufficient understanding of the basics and to be able to fully combine them, and analyze and synthesize process flowsheets. Note that this is in contrast to Process Safety that can be integrated earlier. To avoid any problems in this regard, we recommend that Process Security be integrated primarily into the senior process design and process safety courses, so as to maximize the impact per time ratio on the students. Short demonstrations about Process Security that rely on the software tool introduced in this work, however, can be carried out at any phase of the curriculum as it allows carrying out a basic analysis without much insight into the details of modeling and optimization.

Note that the same difficulties render Process Security an excellent open-ended project for design and safety courses. The analysis and solution require an understanding of dynamic modeling, conceptual design, a basic understanding of optimization, and beyond that analytical reasoning by the students.

Sample module. The objective of Process Security module in a senior design course is to teach students how to analyze process performance under both normal and abnormal conditions, and create retrofit solutions to compensate for the security vulnerabilities by altering the design of existing units, or adding supplementary units. The scope of a retrofit problem can be adjusted to conceptual idea generation for small projects, or completely integrated into a full-scale design project where process security is added as a third objective in addition to economic and technical feasibility. The first case will be exemplified in the case study section.

THE SOFTWARE

To aid in the instruction of Process Security, we have developed a MATLAB-based tool for educational use. This tool enables application of the Process Security Assessment Theory introduced by Uygun *et al*.[16] with a graphical interface and various reporting tools. The tool enables focusing on the conceptual security problem rather than detailed modeling, if that is the objective of the course. Another important feature is that the software performs an optimization procedure, which is necessary in the specific method employed, "behind the scenes", such that a knowledge of optimization is not necessary for security analysis. This renders the software ideal for undergraduate education, where optimization is usually offered as an optional course by most chemical engineering programs.

For educational use, the software is envisioned as a tool that can perform the security analysis for some typical example cases, where the system parameters can be customized so that different problems can be accommodated. These problems can be utilized as educational modules in related courses. The software can be used for either simple demonstrations of security vulnerabilities in an existing process, or an in-depth process security analysis project that students are asked to analyze a process, and create retrofit solutions to reduce or remove vulnerabilities.

Upon entering the security evaluation program, the user has an option to follow a walk-through demo, which is a default example for demonstration purposes (Figure 1). Another option is to enter a simulation environment where the user may model a specific reaction process. Though future work will involve expanding the capabilities of the security software, the current program is functional only for a non-isothermal CSTR example that will be discussed in the next section.

The software interface is simple and user friendly. If the user runs into some confusion, help boxes are implemented throughout the program, allowing the user to right click on any item, for a brief explanation of the button functionality. Ample information on the theory, a step-by-step walkthrough, and other documentation are provided in the information menu (Figure 2). The case study being analyzed is fully customizable by simply modifying the feed and outlet and reactor parameters, including properties like activation energy, overall heat transfer coefficient, and reactor area (Figure 3).

The software has two main functions, process security assessment and significance analysis. The former is to evaluate a confidence interval on the minimum time to disaster, and the latter enables practical evaluation of the significance for the parameters of system with regard to their effect on minimum time to disaster. The software is also capable of producing graphical representations of the system temperature profile as it escalates towards the disaster boundary.

Instead of presenting a more detailed explanation of the functions, an example problem is analyzed using the software. This shows for possible utilization venues in senior process design and/or process safety courses.

SAMPLE STUDY PROBLEM

Problem Statement

Uygun *et al.*[15] present the following differential equations describing a non-isothermal CSTR, based on modification of an example by Luyben[17] (Figure 4):

$$\frac{dV}{dt} = F_0 - F \tag{7}$$

$$\frac{dV_J}{dt} = F_J^{IN} - F_J^{OUT} \tag{8}$$

$$V\frac{dC_A}{dt} + C_A\frac{dV}{dt} = F_0 C_{A0} - F C_A - V k C_A \tag{9}$$

$$V\frac{dT}{dt} + T\frac{dV}{dt} = F_0 T_0 - F T - \frac{\lambda V k C_A}{\rho C_P} - \frac{U A_H}{\rho C_P}\left(T - T_J\right) \tag{10}$$

$$V_J\frac{dT_J}{dt} + T_J\frac{dV_J}{dt} = F_J^{IN} T_{J0} - F_J^{OUT} T_J + \frac{U A_H}{\rho_J C_J}\left(T - T_J\right) \tag{11}$$

where

$$k = A e^{-E/RT} \tag{12}$$

The system parameters and variable ranges are listed in Table 1. In this example of a security threat, the current control system is assumed not operational, therefore characterizing manipulated variables as disturbances. The reactor temperature (*T*) should be considered as a critical variable, since temperature is the main variable of concern under the possibility of a runaway reaction. It should be noted that the volumetric holdups in the reactor and the jacket, reactant concentration and jacket temperature are also assumed to be “vulnerable” (i.e., they can be modified instantly in a security threat condition) so are treated as disturbances. In fact, only the reactor temperature is assumed to fully follow the governing differential model.

There are two obvious threat situations that would drive the critical variable, and hence the exothermic reaction in this example to disaster conditions. First, redirection or shutdown of the cooling water will result in a decrease in heat removal from the system, ultimately leading to a runaway reaction. In addition, an increase in the reactant concentration could provide similar effects as in the first situation, granted higher concentrations of the reactant are available at the plant.

Tasks

Perform a Process Security Assessment study using the software. These are specific questions to answer:

Q1. Is the Process Secure?

Q2. At what temperature does the temperature runaway begin?

Q3. Which variables do have a large impact on the Minimum Time to Disaster?

Q4. Suggest multiple retrofit scenarios for the reactor to reduce vulnerability, outline your reasoning, and discuss the effect of your proposed change.

Solution

The example stated above corresponds to the demo case in the software, and is also the default values in the simulation environment. As such, modification of parameters is not necessary.

As specified earlier, the software comprises two main functions. The first, Security Assessment enables evaluation of a confidence interval for minimum time to disaster. Again, this interval represents the time it would take during a security threat situation, to proceed from the nominal operation to a disaster condition, considering the worst-case scenario. This time range will give the user an understanding of the overall security of their reactor. Choosing this function opens the Security Assessment window, which, upon clicking the start button, makes the necessary calculations for evaluation of the confidence interval (Figure 5).

Answer to Q1. *The confidence interval of the MTD is between 1.5 seconds and 67.4 seconds. Obviously, this time is too short for any reaction. The process clearly presents a security vulnerability. The upper bound time limit would have to be more along the line of minutes or even hours, rather than seconds, in order for the security threat to be reasonably eliminated.*

It is also possible to graphically depict the system moves from the nominal operation to disaster. Actually, there are two figures, first representing the transition that yields the lower bound in the confidence interval, and the latter corresponding to the upper bound.

Answer to Q2: *The transition to disaster is displayed in Figures 6 and 7. The exponential behavior starts around 360 K for the upper bound and 450 K for the lower bound. The actual response will be somewhere between these two curves. Choosing the earlier one, it can be stated that runaway reaction begins at 360 K.*

Answer to Q3: *The second facet of the security evaluation process consists of the generation and analysis of the priority list, which gives the significance and percent significance of each reactor variable (Figure 8). For the given non-isothermal CSTR example, it is shown that the two variables with the highest percent significance, and hence the highest effect in sending the process to disaster during a security threat, are the jacket temperature at just over 70% and the volume of liquid in the reactor at about 25%. Significance analysis is quite important in that it illustrates the variables that need to be monitored closely at all times. If a given variable has a low percent significance, it therefore has a low effect on the temperature runaway.*

Answer to Q4: *The significance values hint the first clue by pointing out high significance values for jacket temperature and reactor volume: the heat from the jacket is instrumental in kick-starting the runaway reaction, whereas a low* *volumetric content in the reactor significantly increases the heating rate. Consider changing the coolant and jacket design such that it would start evaporating at 400 K (Figure 9) and yet would not create a significant pressure buildup in the jacket. The new analysis yields the MTD between 6.4 seconds and 72 seconds. Now consider diluting the reactant feed stock by 50 % such that the maximum feed concentration is halved to 8.01 kmol/m^3. A new analysis yields the MTD between 9.2 seconds and 150.4 seconds. Although we have easily doubled the MTD, this is not sufficient to render the system secure. Other modifications are possible but similarly do have limited effect. As such, the system displays an inherent vulnerability that cannot be eliminated by a simple retrofit of the reactor.*

CONCLUDING REMARKS

Process security addresses the most critical issues in process safety, as it concerns completely unexpected occurrences and extreme severity of process safety problems. As an integrated part of homeland security, process security must be completely assured. To fully prepare engineers with security knowledge, the authors propose to vertically integrate the undergraduate curricula upon the theme of process security.

This paper has introduced a tool that may be implemented in undergraduate process design and/or process safety courses to aid in the incorporation of simple but illustrative examples of the essential nature of process security in a chemical engineering curriculum. This development is a quantitative tool based on the dynamics of a system, which arise when the process experiences various disturbances that may be set by saboteurs who may have sufficient technical background. The software will be made available for instructors of the relevant chemical engineering courses, upon written request to Professor Yinlun Huang.

AKNOWLEDGMENTS

This work is in part supported by the National Science Foundation under grants CCLI-0127307, CTS-0211163, DGE-9987598, and CTS-0407494.

REFERENCES

1. Lemley, J. R., V. M. Fthenakis, and P. D. Moskowitz, "Security Risk Analysis for Chemical Process Facilities," *Process Safety Progress*, **22**(3), 153 (2003)
2. Baybutt, P., "Cyber Security Vulnerability Analysis: An Asset-Based Approach," *Process Safety Progress*, **22**(4), 220 (2003)
3. Lou, H. H., R. Muthusamy, and Y. L. Huang, "Process Security Assessment: Operational Space Classification and Process Security Index," *Trans. IChemE. Part B. Process Safety and Environmental Protection*, **81**(6), 418 (2003)
4. Center for Chemical Process Safety, *Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites*, AIChE, New York, NY (2002)
5. Hendershot, D. C., "Designing for Safety in the Chemical Process Industry: Inherently Safer Design." *Accident Precursors Workshop: Linking Risk Assessment With Risk Management*, July 17-18, 2003, Washington, DC, Washington, DC: National Academy of Engineering, 2003.
6. Crowl, D. A. and J. F. Louvar, *Chemical Process Safety: Fundamentals with Applications*, 2nd ed., Prentice-Hall, Upper Saddle river, NJ (2002)

7. Center for Chemical Process Safety, *Inherently Safer Chemical Processes – A Life Cycle Approach*, AIChE, New York, NY (1996)

8. Center for Chemical Process Safety, *Guidelines for Chemical Process Quantitative Risk Analysis*, 2nd Ed., AIChE, New York, NY (2000)

9. Center for Chemical Process Safety, *Layer of Protection Analysis, Simplified Process Risk Assessment*, AIChE, New York, NY (2001)

10. Dimitriadis, V. D., J. Hackenberg, N. Shah, and C. C. Pantelides, "A Case Study in Hybrid Process Safety Verification," *Computers Chem. Engng*., **20**, Suppl., s503 (1996)

11. Mannan, M. S., A. Akgerman, R. G. Anthony, R. Dabby, P. T. Eubank, and K. R. Hall, "Integrating Process Safety into ChE Education and Research," *Chemical Engineering Education*, **33**(3), 198 (1999)

12. Cunningham, S., "What Can the Industrial Chemical Community Contribute to the Nation's Security," presented at the *Workshop on National Security & Homeland Defense: Challenge for the Chemical Science in the 21st Century*, National Academies of Sciences and Engineering, Irvine, CA, Jan. 14-16, 2002.

13. Margiloff, I. B., "Geopolitics and Chemical Engineering," *Chem. Eng. Prog*., **97**(12), 7 (2001)

14. Ragan, P. T., M. E. Kiburn, S. H. Roberts, and N. A. Kimmerle, "Chemical Plant Safety: Applying the Tools of the Trade to a New Risk," *Chem. Eng. Prog.*, **98**(2), 62 (2002)

15. Uygun, K., Y. L. Huang, and H. H. Lou, "Process Security Analysis: γ-Analysis and Σ-maps," *AIChE J*., **49**(9), 2445 (2003)

16. Uygun, K., Y. L. Huang, and H. H. Lou, "Fast Process Security Assessment Theory," *AIChE J*., **50**(9), 2187 (2004)

17. Luyben, W., *Process Modeling, Simulation and Control for Chemical Engineers*, 2nd ed., McGraw Hill, New York, NY (1990)

Table 1. Variable Ranges and Parameters

Variable name	Minimum	Nominal	Maximum
Reactor Feed Flowrate (F_0) (m^3/h)	0	1.13	1.98
Reactor Output Flowrate (F) (m^3/h)	0	1.13	1.98
Jacket Feed Flowrate (F_J^{in}) (m^3/h)	0	1.41	2.83
Jacket Output Flowrate (F_J^{out}) (m^3/h)	0	1.41	2.83
Reactor Feed Temperature (T_0) (K)	222.22	294.44	555.56
Temperature in Reactor (T) (K)	222.22	333.33	555.56
Temperature in Jacket (T_J) (K)	222.22	330.33	555.56
Inlet Concentration (C_{A0}) (kmol/ m^3)	0	8.01	16.02
Concentration (C_A) (kmol/ m^3)	0	3.92	16.02
Volume of liquid in reactor (V) (m^3)	0.02	1.36	1.98
Coolant Volume in Jacket (V_J) (m^3)	0.002	0.11	0.198
Parameters			
Jacket Feed Temperature (T_{J0}) = 294.44 K	Cp = 3.14 kJ/ kg K		
E = 69,780 kJ/ kmol	ρ = 800.95 kg/m^3		
U = 3,066.3 kJ/h m^2 K	C_J = 4.19 kJ/ kg K		
A_H = 23.23 m^2	ρ_J = 997.98 kg/m^3		
R = 8.314 kJ/ kmol K	λ = -69,780 kJ/ kmol		
α=7.08 10^{10} h^{-1}			

LIST OF FIGURES

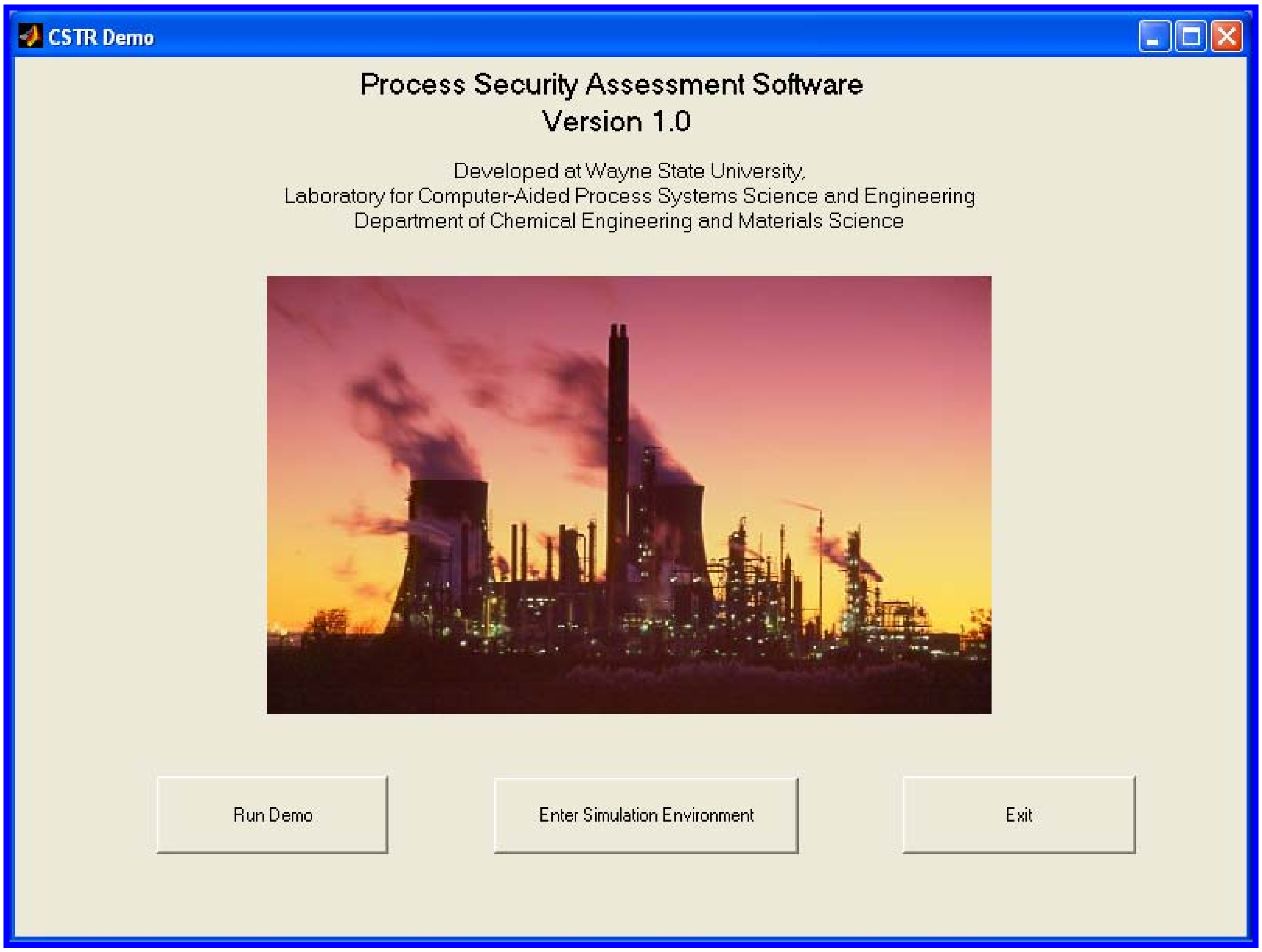

Figure 1. Process Security Assessment Tool – Main Window.

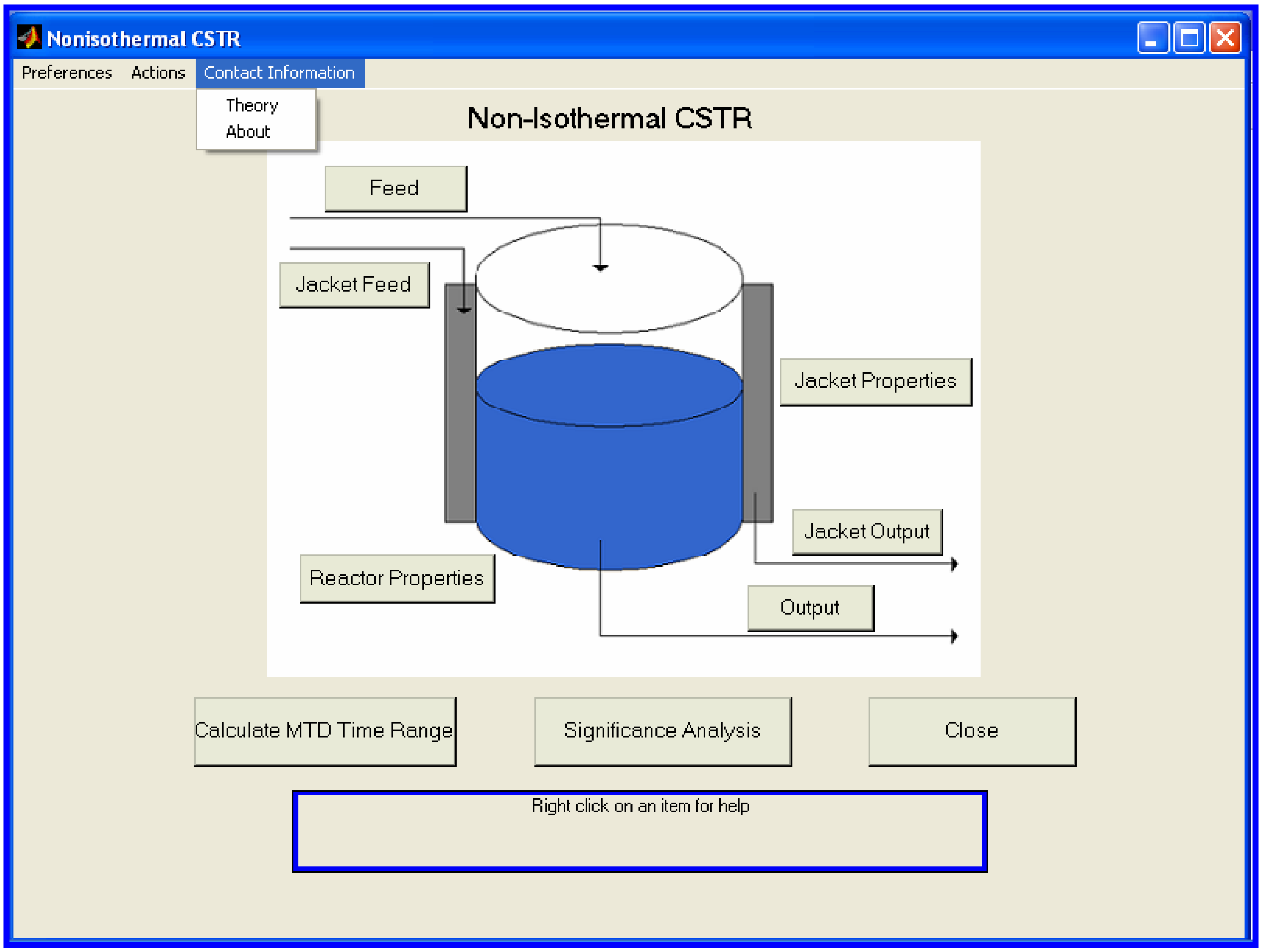

Figure 2. Process Security Assessment Tool – Non-isothermal CSTR example.

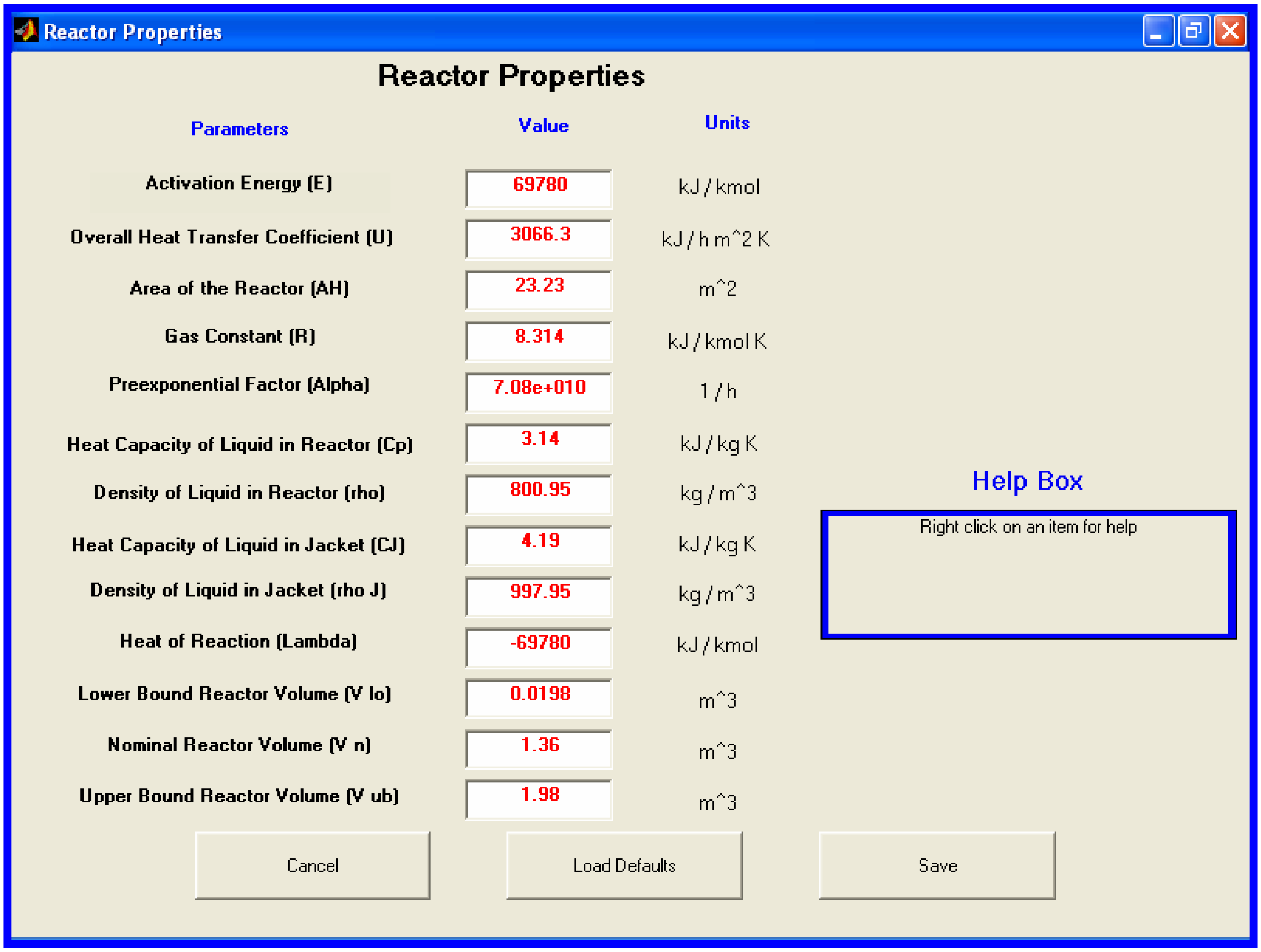

Figure 3. Non-isothermal CSTR example – the Reactor Properties window.

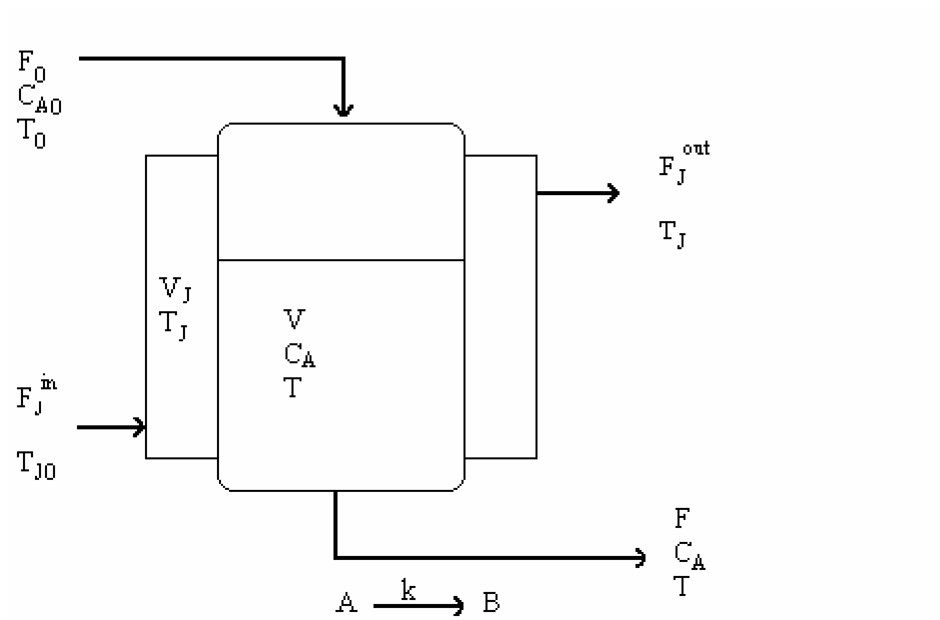

Figure 4. Non-isothermal CSTR with a cooling jacket.

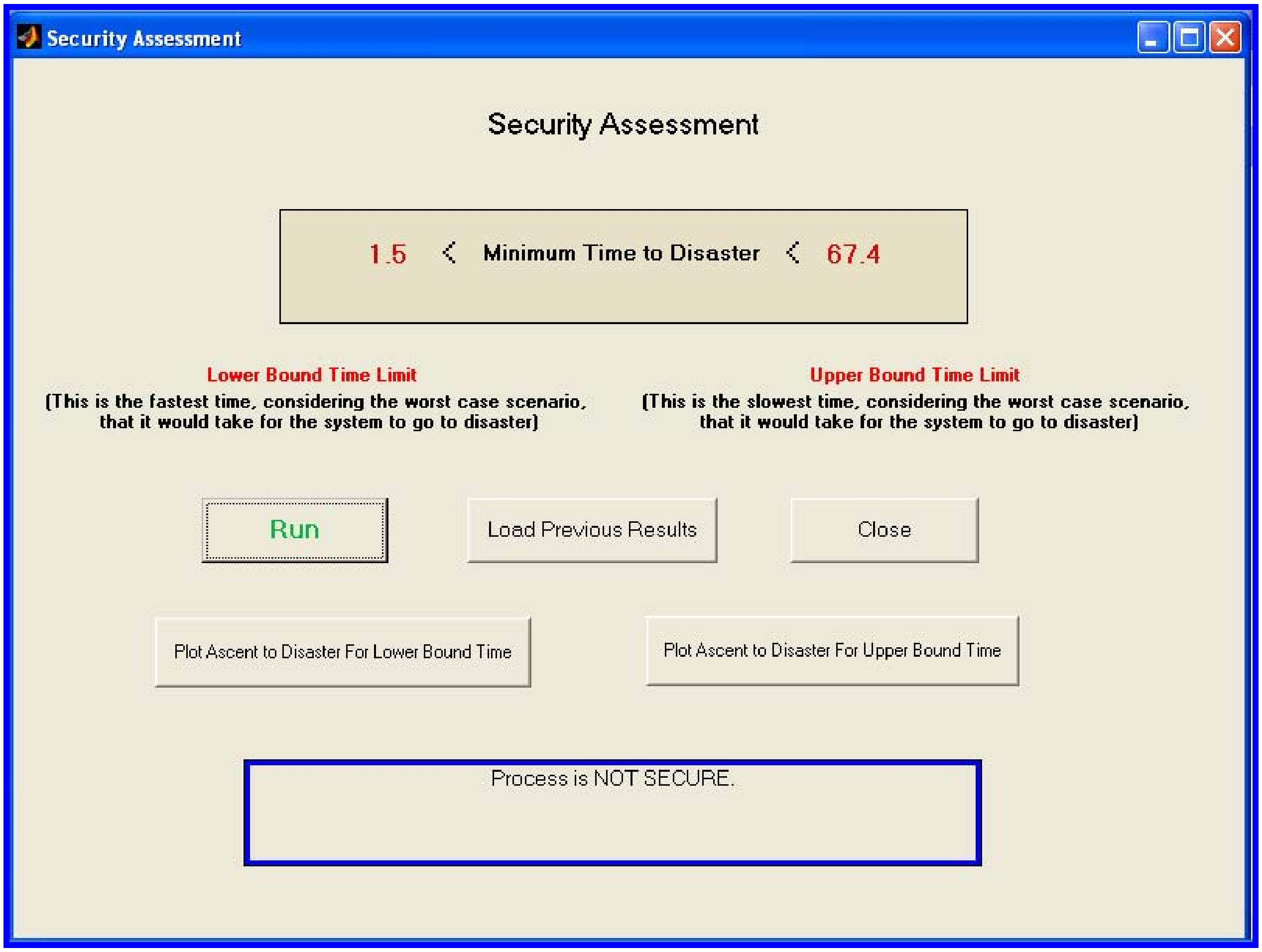

Figure 5. Minimum Time to Disaster (MTD) calculations
for the non-isothermal CSTR problem.

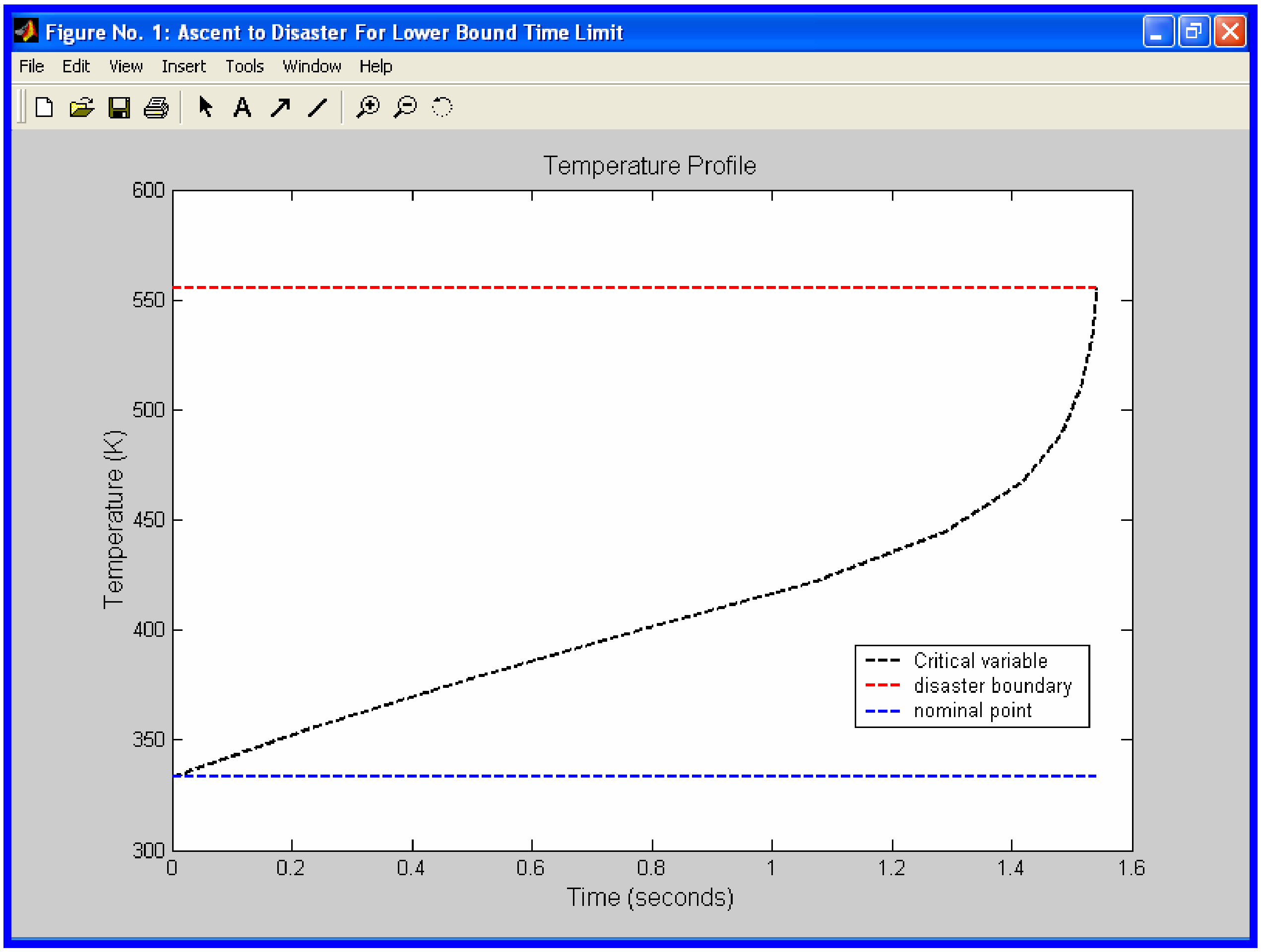

Figure 6. Temperature Profile for the Lower Bound Time to Disaster.

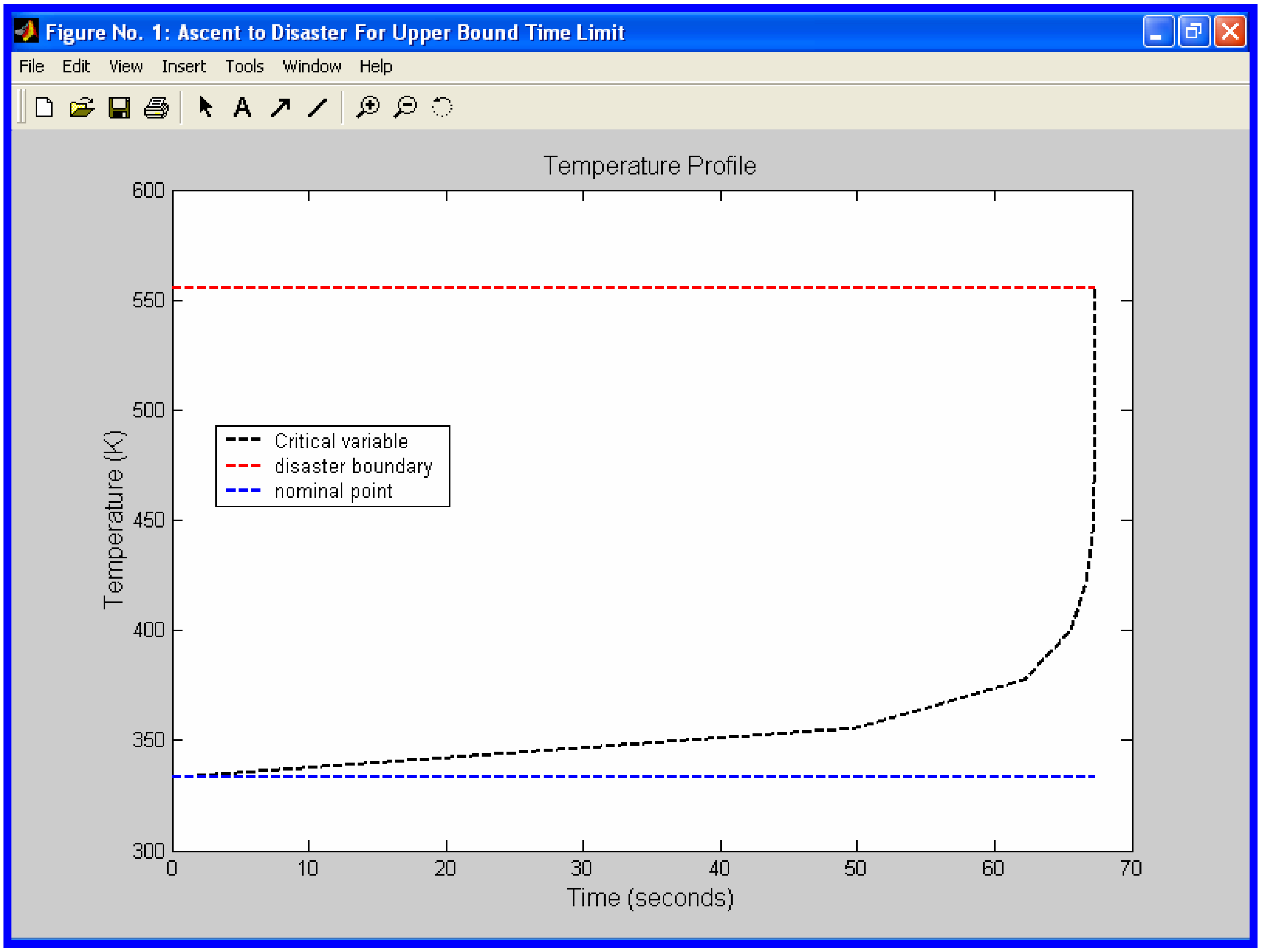

Figure 7. Temperature Profile for the Upper Bound Time to Disaster.

Figure 8. Process security assessment – Priority List.

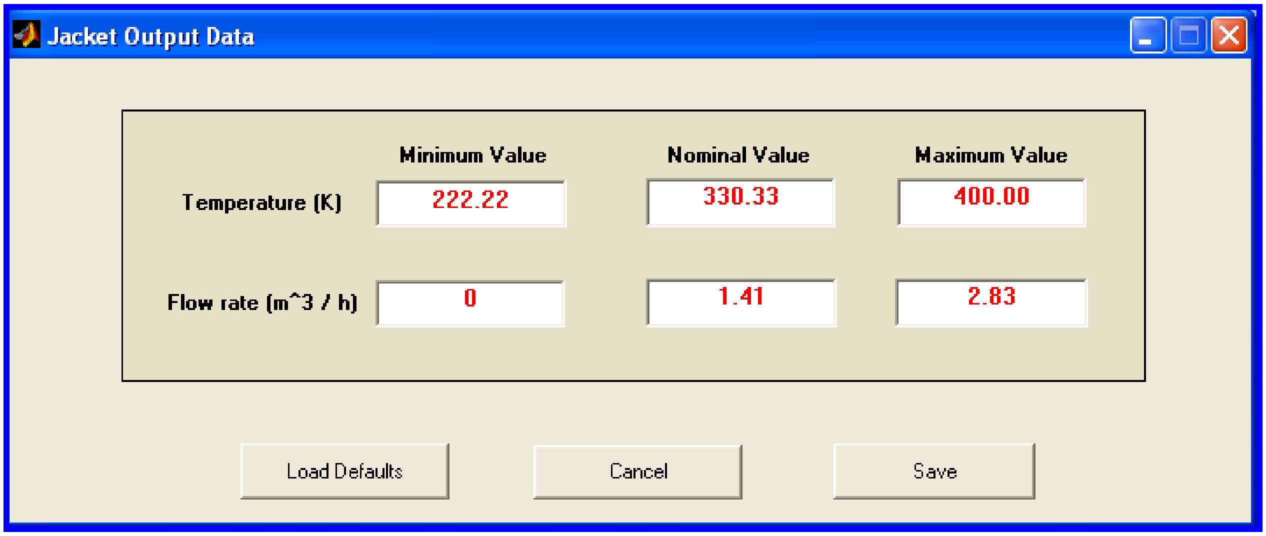

Figure 9. Altered coolant properties.

Cristina Piluso received her BS degree in Chemical Engineering at Wayne State University in 2003. She has won many awards and was a Wayne State University Presidential Scholar between 1998-2003. She is currently an NSF-IGERT fellow and a PhD student working with Professor Yinlun Huang on process security assessment and decision making using advanced computing methods.

Korkut Uygun received his BS and MS in Chemical Engineering from Bogazici University, Turkey, and his PhD from Wayne State University. He is currently a post-doc with Prof. Yinlun Huang and part-time faculty in Wayne State Dept. Chem. Eng. & Mat. Sci., and has recently introduced a fast security assessment theory for chemical processes. Research interests include mixed integer dynamic optimization, non-linear MPC, process systems engineering, sustainable engineering, and systems biology.

Yinlun Huang is Professor in the Chemical Engineering Department at Wayne State University. He received his BS from Zhejiang University, China, and MS and PhD from Kansas State University, all in Chemical Engineering. He teaches process and product design, chemical process integration, and advanced engineering mathematics. His research interests are in process systems science and engineering, information processing and decision making, computational biology, and sustainable engineering.

Helen H. Lou is Associate Professor in the Chemical Engineering Department at Lamar University. She received her BS ChE from Zhejiang University, China, and MS ChE, PhD ChE, and MA Comp. Sci. from Wayne State University. Her research and teaching interests are mainly in the areas of process synthesis, modeling, control, and optimization, information technology, and industrial sustainability.