Proceedings of the 2015 Industrial and Systems Engineering Research Conference
S. Cetinkaya and J. K. Ryan, eds.

Integrated Systems Engineering and Economic Analysis Models For High Reliability Operations

Kurt F. McElwain
CNS Pantex
Amarillo, Texas

Michael W. Bromley
CNS Pantex
Amarillo, Texas

Dr. Jaime Cantu
Texas Tech University
Lubbock, Texas

Dr. Mario G. Beruvides
Texas Tech University
Lubbock, Texas

Abstract

Commonly used risk models tend to be static and do not incorporate the feedback of an operating environment. Engineers/Stakeholders are left in the position of being caught between the ideal of reducing risk to the lowest possible level and the reality of having to pay for the barriers and controls that reduce risks. High hazard industries such as high explosives manufacturing operations need a methodology for integrating feedback, economics and risk. The systems analysis being proposed uses causal loops to represent feedback, 20-year life cycle analysis to estimate economic costs and an existing hazard analysis with published risk factors. The model implies that a strong response to weak signals is cost effective and valuable for preventing catastrophic events. The resulting methodology successfully demonstrates that risk and cost models can be linked using systems tools to yield improved decision making.

Keywords
Causal loops, Feedback, System Safety, Risk Analysis, Safety Costs

1. Introduction

The research presented in the following paper is an on-going research project initiated in the year 2011. With the help of a Plant Directed Research and Development (PDRD) grant from the Department of Energy (DOE), researchers investigated how High Reliability Organization (HRO) theory could be put into practice at the Pantex Plant in Amarillo, Texas to optimize safety barriers and controls and their economic efficiency. The Pantex Plant is the final assembly and disassembly point for nuclear weapons and the development, formulation, manufacture and testing of high

explosives (HE), a mission requiring high reliability operations. This mission is performed under the direction of the NNSA Production Office (NPO) of the National Nuclear Security Administration (NNSA).

HRO theory postulates that endless accident-free operations are possible, but the application of the theory to actual operations and processes is still developing as an ongoing process. Texas Tech University (TTU) researchers and CNS Pantex personnel examined an actual highly hazardous operation. They used a systems engineering approach and tools such as process flow diagrams, stock and flow diagrams, process hazards analysis, causal loop diagrams, risk analysis, cost engineering and economic analysis techniques for this. The intent was to build an integrated systems dynamic and economic analysis model directly applicable to the case study process, yet potentially transportable to other highly hazardous operations. [1]

The researchers realized after a thorough review of the literature that the basis of existing HRO research was mainly qualitative, not quantitative in nature. The tools within the literature used primarily static, rather than dynamic analysis methodology and techniques. HROs operate in complex, hazardous environments requiring very effective barriers and controls to prevent unfavorable events. Therefore the team believed that the problem was the lack of an integrated systems dynamic and economic model using probabilistic methods to analyze barriers and controls used in highly hazardous operations. To complicate matters more, there are multiple variables, costs and complex interrelationships between variables. This comprehensive dynamic model would provide a mathematical and scientific technical basis for benefit/cost based decisions on safety barriers and controls. The model would be essential to the development of high reliability operations to more accurately select barriers and controls that are efficient as well as cost effective. [2]

The exploratory research project was completed in 2013 and succeeded in demonstrating that integrated systems dynamic and economic analysis models can help determine efficient, cost effective barriers and controls for a complex, highly hazardous process. The team specifically proved quantitatively that for every order of magnitude of risk reduction there is a range of costs for various combinations of a given baseline set of barriers and controls. It was discovered that the integrated systems dynamic and economic analysis modeling technique could make a positive impact on management decisions. Thus the model on safety and cost should be further explored due to the potential for significant cost reductions with limited levels of safety reduction. [3]

In 2014 a follow up PDRD grant allowed the team to continue the initial research started three years earlier. Further, it was discovered that the systems dynamic modeling technique has great potential to assist management in decisions with respect to safety/cost administration for hazard analysis that was not pursued under the scope of this research project. Future research opportunities are outlined in the report [4]

2. Methodology

Figure 1 defines a framework for putting HRO theory into practice. The process to be analyzed is a bonding operation between two High Explosive (HE) components. The first step is to review the current operating procedures or process flow diagram and create a process flow diagram. The diagram was created in conjunction with operations personnel and reviewed by all personnel at the

end to ensure accuracy. The personnel interviewed were process engineers or operations personnel and were interviewed separately to ensure that both the process as envisioned and designed and the process as executed are factored into the model. The second step was to review the process from the perspective of hazards to the HE that exist in the process. The hazard focus is on the prevention of accidents, particularly accidents called pinnacle or plateau events. A Preliminary Hazard Analysis (PHA) was performed for this operation. It is necessary to ensure the PHA is bounding for all potential hazards inherent in the process. The validation that the PHA is complete was the next step of the process.

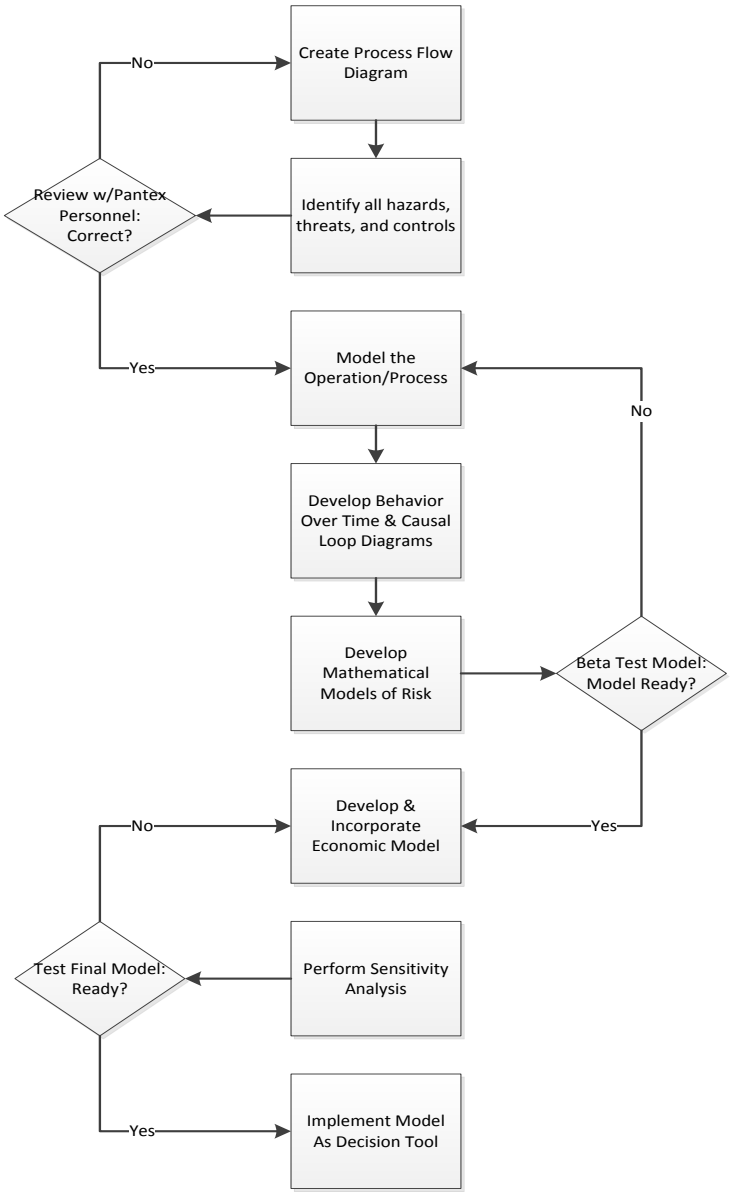

Figure 1: Project Methodology Flow Diagram

In order to identify all hazards, threats, and controls the research team categorized the adverse or unfavorable events into four levels based on the level of destruction to human beings, physical assets, the company or the environment should all barriers and controls fail and the unfavorable event becomes a reality. It is critical for analysts and management to understand these event categorizations. These four levels are the Level 4 Event, the Level 3 Incident, the Level 2 Plateau Event, and the Level 1 Pinnacle Event.

For economic analysis purposes, the analyst must determine or be given the duration of the life of the project or program to be analyzed. This is important to the analysis because almost all hazardous operations require facilities and equipment to be designed, constructed and provided. These facilities and equipment have costs, and benefit-to-cost analysis of alternatives for these items requires time value of money analysis, which requires a duration in years to accomplish.

In order to probabilistically estimate the costs of events, incidents, Plateau Events and Pinnacle Events, it was necessary to pull significant amounts of data from several databases of the Pantex Plant, which were searched to find out the annual probabilities of the four categories, or levels, of events.

2.1 Behavior Over Time & Process Flow Diagrams

A process flow diagram was the first tool the team used was to investigate and expose critical safety points and pinpoint important cost drivers. The first step in analyzing the process is to define the process (systems) flow diagram. It is critical for the diagram to be accurate. This is not always as obvious as it might seem to be as "it is fundamental for resilience engineering to monitor and learn from the gap between work as imagined and work as performed" [6]. The process was first laid out by the Process Engineers. It was then walked down by the researchers as it was actually performed by production personnel. The production personnel then reviewed the process flow diagram for accuracy. The multiple points of view (process engineers, technicians and the observing researchers) reviewing the diagram bridged the gap between work as imagined and performed. The differences between the two were not significant for this process but could be in other circumstances.

2.2 Causal Loop Diagrams

Causal Loop Diagrams (CLD) were used to show the interrelationships and dependencies between variables and how they affect each other. These were developed for each of the relevant risk scenarios. A generic causal loop diagram was developed that incorporated a suite of standard barriers and controls for highly hazardous operations and processes. Detailed CLDs were developed for several scenarios and were discussed with CNS Pantex line personnel to determine if the level of detail is a factor in the accuracy of the systems dynamic and economic models. It is useful for future modeling efforts, and in preparation for developing the integrated model, to understand the level of detail that will provide the best result. Detailed models are more expensive to develop and maintain, and become more complex to handle, and therefore more prone to error. The optimum level of detail to create a reliable and stable model was a key aspect of this research project. The principal activities to construct the individual CLDs were as follows:

- Obtain Written Process/Engineering/Administrative Control Documents
- Conduct Employee Interviews

- Observe the Operation/Process (where permissible for TTU researchers)
- Identify Hazards, Threats and Controls for the Operation/Process
- Develop Behavior over Time (BOT) Graphs
- Develop Causal Loop Diagram (CLD)

Once the CLDs were created a systems dynamic model was created using Vensim Systems Dynamic software, and integrated with the economic model.

2.3 Program/Process Life

The analysis of alternatives must include the time value of money and discounted cash flow analysis techniques. The life of the project affects the total costs of the project due to the time value. Twenty (20) years is a common life of a project used for benefit-to-cost analysis because that is the length of time it takes for most facilities and equipment to wear out. If a facility or equipment last longer, the analyst should use that value for the analysis.

2.4 Unfavorable Event Categorization

The four levels of unfavorable events proposed by this research team follow:

- Level 4 Event: A Level 4 event is something adverse or unfavorable, not involving injuries or property damage, that could impact the safety or security of people, property, national assets or the environment, and should be investigated and prevented if possible.
- Level 3 Event: A Level 3 event is called an Incident. An incident is an adverse or unfavorable event with injuries and/or property damages and/or environmental damages that could shut down the organization for a short period of time. An incident requires reporting to the authorities, immediate investigation, more intense root cause analysis, and formal corrective actions to prevent future reoccurrence
- Level 2 Event: A Level 2 event is called a Plateau Event. Expanding on Hartley's definition, a Level 2 Plateau Event is an accident with any of the following: serious injuries, fatalities, major property damage, environmental damages, or national security asset damage. Emergency safety and security personnel mobilize to the site. Operations and possibly the plant shuts down while reporting, investigations, analysis and corrective actions are developed and deployed. [6]
- Level 1 Event: A Level 1 event is a Pinnacle Event: Again expanding on Hartley's definition, a Level 1 Pinnacle Event is the worst possible accident, involving multiple injuries or fatalities to personnel and major damage to property, the environment and national security assets. Emergency safety and security personnel mobilize to the site. Operations and the plant shut down for many months or years while reporting, investigations, analysis and corrective actions are developed and deployed.. [6]

2.5 Cost Estimating Principles

Cost estimating was required on three areas; facility requirements, process requirements, and the costs of the unfavorable events should there be a failure of facility or process barriers or controls. Cost drivers for the facility and process requirements included USDOE Orders, standards and guidelines, industry codes and standards, Plant Standards and operating Procedures, and special requirements of Subject Matter Experts in the hazard field. The costs for unfavorable events were developed through study of Level 1 through Level 4 events at the Plant site. The Plant events are

fairly well captured in official reporting systems, and with some sorting work the categorization into the four event levels is possible, and the annual probability is calculable. A scenario analysis technique as well as plume studies assisted with the determination of what transpires in our current regulatory environment when bad events happen. The breakdowns of the scenarios enabled detailed cost estimates to be developed to reflect those realities.

In order to sum and compare the costs of barriers, controls and unfavorable events, Discounted Cash Flow analysis (formula 1) was used with 20 years estimate for the life of the operation.

$$A = P \times (A|P, i\%, N) \quad (1)$$

Where A is the yearly amount of the annuity, P is the Present or Initial costs, "i" is the interest rate, and N is the number of years included in this study. This value is the comparative cost for barriers, controls and adverse events. [7]

3. Results

The use of systems engineering and techniques for the analysis of the highly hazardous process combined with the engineering economics alternatives analysis techniques resulted in an integrated model that can determine the most efficient and cost effective suite of barriers and controls for a highly hazardous operation. A portion of the actual Process Flow Diagram for the process analysis is shown below.

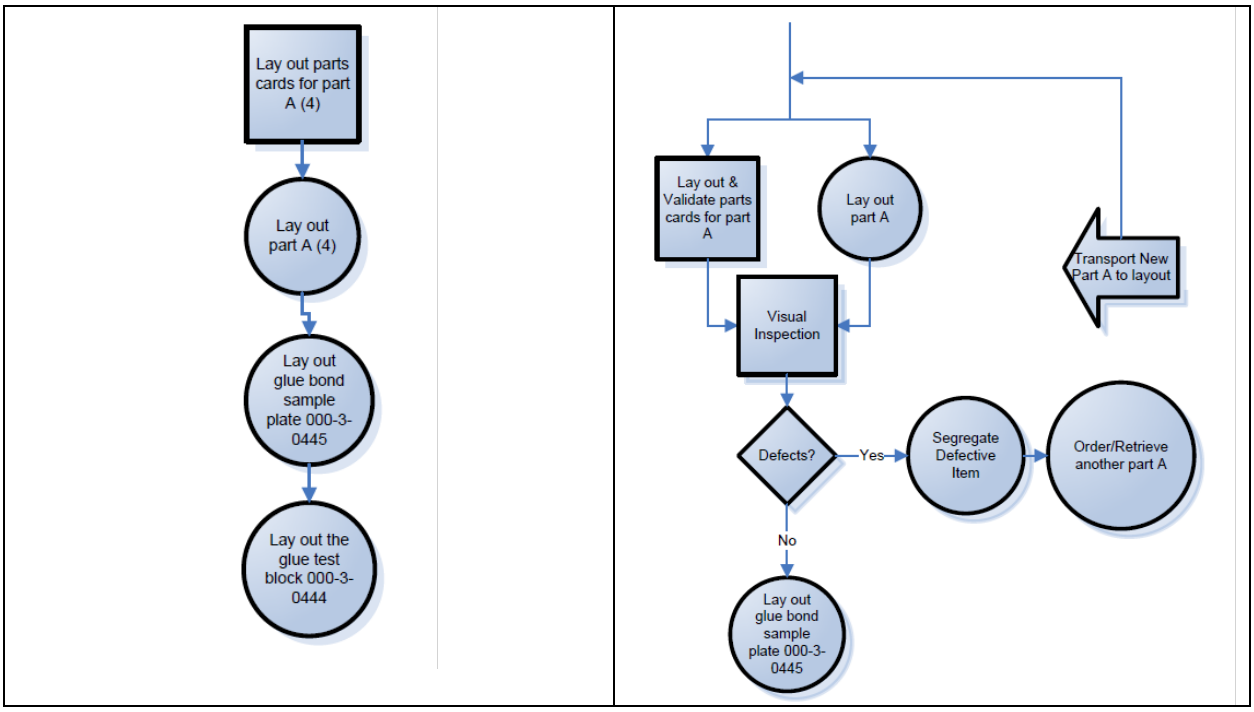

Figure 2: Management Perceptions (Left) & Line Workers Perception (Right)

For example, Figure 2 (Left) shows managements perception of the start of an HE operation. Management perceived that temperature and humidity checks were made, materials were delivered and the assembly started in one day. Figure 2 (Right) shows line workers perception that the start of HE operations is three to seven days earlier than management. Technicians check inventory, order necessities, schedule the transportation of materials and ensure the building HE limits are not exceeded. Then temperature and humidity controls are validated and assembly would start. Both management and line workers were correct on the assembly process but their perceptions of where the operations start differed. Perceptions between management and line workers may seem minor but are important to understanding the process.

The systems dynamic portion of the model helped the researchers determine the suite of barriers and controls that optimize the safe operation of the process. One of the most insightful tools and techniques used for the barrier and controls analysis was the Causal Loop Diagram. This is a common systems engineering technique used to point out the influences and the relationships between various parameters and variables.

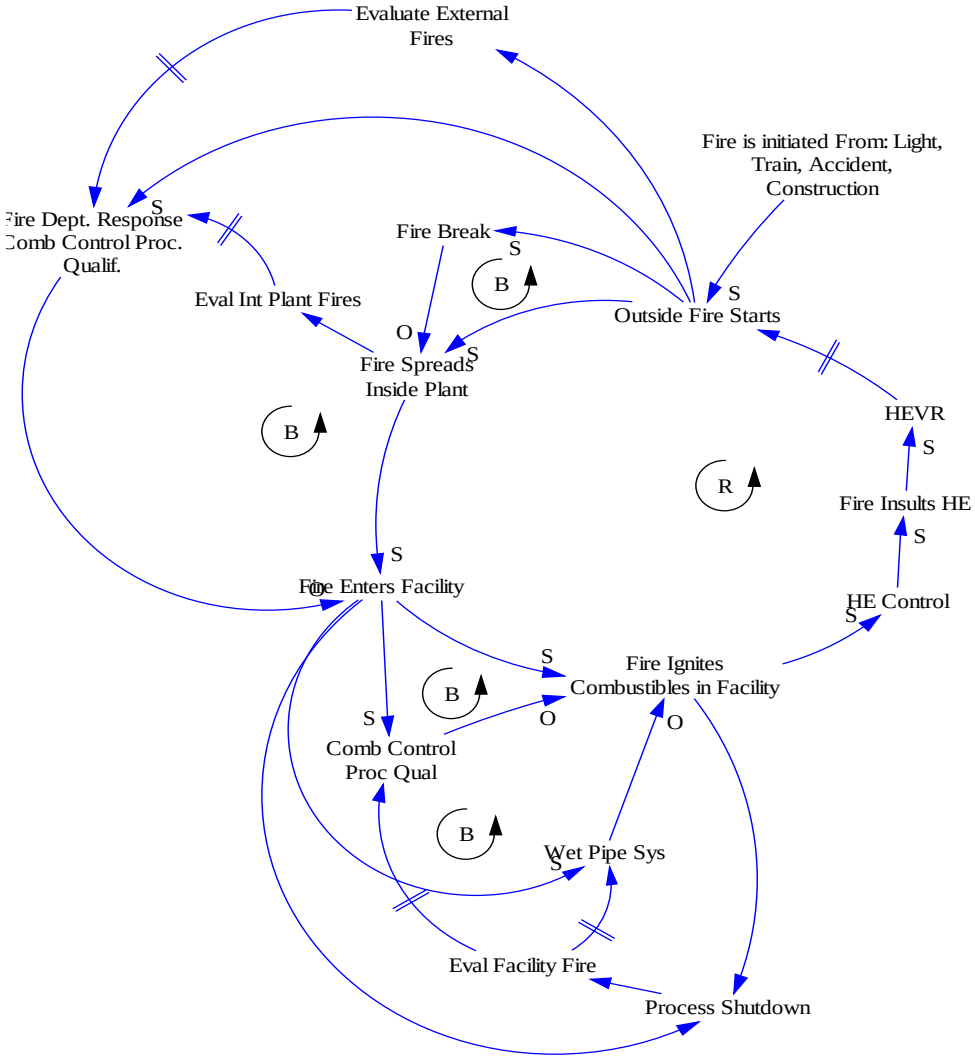

Figure 2: Example Causal Loop Diagram for One Scenario

Using a Causal Loop Diagram to model one of the scenarios considered to be feasible, it can be seen that if a spark led to a fire in the bay of the subject operation, the accident would not be a Level 4 Event nor a Level 3 Incident. It would be a Level 1 Pinnacle Event if the worst thing happened (an explosives detonation). That event would shut down operations and potentially the plant for a very long time. If the second worst thing happened, a Level 2 Plateau Event (fire stopped before an explosives detonation), the operation and possibly a portion of the plant would be shut down long enough for intensive investigation and corrective action development and implementation. The economic analysis portion of the model enabled them to form a very important principle for HROs.

The principle is that "all barriers and controls with total annualized costs less than the annualized cost of the unfavorable event they are supposed to prevent or mitigate are economically efficient, and therefore value-added. However, barriers and controls having total annualized costs greater than the annualized cost of the unfavorable event they are supposed to prevent/mitigate are economically inefficient and therefore non-value-added, and should be eliminated."[5] The development of cost estimates for barriers and controls begins with a review of any previous documentation for the process, in this case the Process Hazards Analysis, to see what barriers and controls are required and if there are any feasible alternatives. By detailed breakdown of the Process Flow Diagram, the analysts were able to determine if any barriers or controls were left out, if there are any that don't reduce risk or if there are any new that would reduce risk. Then they checked if there is potential for incorporating Lessons Learned (LL) or Continuous Improvement (CI) into the barriers or controls. Checklists were used to reduce errors and omissions.

The Administrative Controls (AC) in this case were Procedures and Training. Every AC must be conceived or directed, planned, developed, documented, taught, learned and continuously improved by a team of people usually known as Subject Matter Experts. Development of Engineered Barriers and Controls is very similar, but they are conceived, designed, developed, documented, drawn up, specified, constructed, tested and put into service primarily by engineers. All costs for the barriers and controls were estimated with input from previously executed projects having actual historical costs. Those that required construction, such as Fire Suppression Systems, were estimated using the industry standard cost estimating reference manual, RS Means. All barriers and controls have initial development costs, ongoing maintenance and repair costs, and terminal 6D costs (Deactivation, Decommissioning, Design, Decontamination, Demolition, and Disposal) if they are in a physical form.

For capturing the costs of the Level 1 through Level 4 events, scenario analysis was used based on the reactions in the past history to these types of events. The costs of Level 1, 2, 3 and 4 events are very important for the analysis. For the subject highly hazardous operation, Level 4 and Level 3 event costs are very low, in the $10-20,000 range, but their frequency is very high. The Level 2 Plateau event costs were in the range of $100,000 and involved some plant shutdown. The Level 1 Pinnacle event costs were over 100 times the Plateau event costs because they require extensive government agency participation, a long plant shutdown, idle workers and extensive corrective actions. As the severity of the events escalated, resulting costs increased geometrically. The final step required comparing the annualized costs of barriers and controls to the annualized costs of the

Level 1-4 event. A barrier or control having annualized costs less than the probabilistic event scenario costs is considered to be cost effective.

The economic analysis portion of the model enabled them to form a very important principle for HROs. The principle is that all barriers and controls with total annualized costs less than the annualized cost of the unfavorable event they are supposed to prevent or mitigate are economically efficient, and therefore value-added. However, barriers and controls having total annualized costs greater than the annualized cost of the unfavorable event they are supposed to prevent/mitigate are economically inefficient and therefore non-value-added, and should be eliminated." [4]

The final step required is comparing the annualized costs of barriers and controls to the annualized costs of the Level 1-4 event. A barrier or control having annualized costs less than the probabilistic event scenario costs is considered to be cost effective. Table 1 is just one example out of many economic analysis summary tables developed by the researchers for various scenarios, which illustrates the estimated costs associated with safety barriers and controls for one accident scenario of one highly hazardous operation. The estimated costs associated with the failure of these barriers and controls is listed as an order of magnitude as compared to the costs of the barriers and controls.

Table 1: Barrier and Unfavorable Event Costs in the Short-to-Fire Scenario

Barrier/Control/Event	**Cost Effective**	**Cost Order of Magnitude**
Procedures	Yes	1.0
Worker Training and Qualification	Yes	1.0
Fire Suppression Systems	Yes	1.0
Fire Detection and Alarm System	Yes	1.0
Event	-	NA
Incident	-	NA
Plateau Event	-	15
Pinnacle Event	-	1,800

In Table 1 it is clear that the failure of barriers and controls that prevent a Pinnacle Event would result in extraordinary costs, approximately 1,800 times more costly than any of the barriers and controls (this results in cost values in the tens of millions of dollars). This reality makes one realize that the Fire Suppression System, which could prevent this Pinnacle Event, is so very cost effective. These costs were developed from the initial construction or development costs, annual maintenance costs, and the 6D costs at the end of the life of the operation (deactivation, decontamination, decommissioning, design, demolition, and disposal). This illustrates the enormous costs incurred by the plant and society if the barriers and controls fail and the worst and next to worse scenarios come to reality.

4. Conclusions

One of the principles of HRO is the idea that management should show a very strong response to weak signals from highly hazardous processes and operations. The 3-year long effort of this research team is exactly that. The team's pursuit of high reliability operations and better decision-making for safety, reliability and cost effectiveness of highly hazardous operations is believed to be itself a cost effective endeavor due to several discoveries related to the operation which point to deficiencies or areas for improvement of the safety envelope at very low cost. Of course, some areas of improvement were not so inexpensive. The subject hazardous process was analyzed to a level of detail not normally performed at the plant because it is thought not to be necessary. The end result is believed to be a large step forward in the pursuit of safe, cost effective barriers and controls for highly hazardous processes and operations.

Acknowledgement

Acknowledgement goes to the NNSA for the PDRD grant which funded this research.

References:

1. Bromley, M.W., McElwain, K., Ng, E.-H., Simonton, J., & Beruvides, M., 2011, "High reliability operations: Systems dynamic and economic analysis modeling of B&W (now CNS) Pantex Plant high explosive operations", Annual International Conference of the American Society for Engineering Management, p. 343-349
2. McElwain, K., Bromley, M., Cantu, J., Tolk, J., Patterson, P., Simonton, J., Beruvides, M., 2012, "Using quantitative analysis to establish a basis for high reliability organizations", Annual International Conference of the American Society of Engineering Management, p. 797-805
3. Beruvides, Mario, Tolk, Janice, McElwain, Kurt, Bromley, Michael, Cantu, Jaime, Patterson, Patrick & Simonton, James, 2013, "High reliability operations: Systems dynamic and economic analysis modeling of CNS Pantex Plant high explosive operations", A Report to the Consolidated Nuclear Security Pantex Plant, Amarillo, Tx
4. Beruvides, Mario, McElwain, Kurt, Bromley, Michael, Cantu, Jaime, 2014, "Systems Dynamic and Economic Analysis", Technical Report submitted by Texas Tech University Industrial Engineering Department Laboratory for Systems Solutions to CNS Pantex Plant, Amarillo, Tx
5. Woods, D D and Hollnagel, E, 2006. "Prologue: Resilience engineering concepts, Resilience Engineering: Concepts and Precepts" (eds: E Hollnagel, D D Woods and N Leveson) (Ashgate Publishing: Aldershot).
6. Hartley, R. S., Tolk, J. N., & Swaim, D. J., 2008, "Introduction to Pantex High Reliability Operations: A Practical Approach to Avoid the System Accident", B&W Pantex, Amarillo, Texas
7. Canada, J.R., Sullivan, W. G., Kulonda, D.J., & White, J.A., 2005, *Capital Investment Analysis for Engineering and Management, 3rd Edition*, New Jersey: Pearson Education