Available online at www.sciencedirect.com
SCIENCE DIRECT
ELSEVIER
Reliability Engineering and System Safety xx (2004) 1–13
RELIABILITY ENGINEERING & SYSTEM SAFETY
www.elsevier.com/locate/ress

Development of a dynamical systems model of plant programmatic performance on nuclear power plant safety risk

Stephen M. Hess[a,*], Alfonso M. Albano[b], John P. Gaertner[c]

[a]*Sensortex, Inc., 515 Schoolhouse Road, Kennett Square, PA 19348, USA*
[b]*Department of Physics, Bryn Mawr College, Bryn Mawr, PA 19010, USA*
[c]*Electric Power Research Institute, 1300 Harris Boulevard, Charlotte, NC 28262, USA*

Received 31 August 2004; accepted 19 October 2004

Abstract

Application of probabilistic risk assessment (PRA) techniques to model nuclear power plant accident sequences has provided a significant contribution to understanding the potential initiating events, equipment failures and operator errors that can lead to core damage accidents. Application of the lessons learned from these analyses has resulted in significant improvements in plant operation and safety. However, this approach has not been nearly as successful in addressing the impact of plant processes and management effectiveness on the risks of plant operation. The research described in this paper presents an alternative approach to addressing this issue. In this paper we propose a dynamical systems model that describes the interaction of important plant processes on nuclear safety risk. We discuss development of the mathematical model including the identification and interpretation of significant inter-process interactions. Next, we review the techniques applicable to analysis of nonlinear dynamical systems that are utilized in the characterization of the model. This is followed by a preliminary analysis of the model that demonstrates that its dynamical evolution displays features that have been observed at commercially operating plants. From this analysis, several significant insights are presented with respect to the effective control of nuclear safety risk. As an important example, analysis of the model dynamics indicates that significant benefits in effectively managing risk are obtained by integrating the plant operation and work management processes such that decisions are made utilizing a multidisciplinary and collaborative approach. We note that although the model was developed specifically to be applicable to nuclear power plants, many of the insights and conclusions obtained are likely applicable to other process industries.
© 2004 Published by Elsevier Ltd.

Keywords: Nonlinear dynamical systems; Process model; Risk management

1. Introduction

Economic and regulatory pressures on nuclear plant operators have resulted in an increased need to explicitly manage safety risk at commercial nuclear power plants. Transition to an open access generation marketplace has forced plant operators to become much more cost conscious and focused on plant performance. The regulatory perspective also is in a state of transition from a command and control framework to one that is risk-informed and performance-based. Due to these changes, both plant management and regulatory authorities need the capability of responding to external constraints while simultaneously ensuring that risk remains at an acceptable level. Because of the relatively static nature of the plant design, changes implemented are predominantly to plant programs and processes. Additionally, age related failure mechanisms provide another stimulus to these programmatic and process changes. Thus, the majority of changes in plant risk are due to these factors; however, these are precisely the same factors that are not adequately addressed by the probabilistic models currently used to analyze them. In a recent and thorough discussion of the current state of the art in the modeling and application of PRA methods to nuclear plant safety, the limitations identified in addressing the impact of human performance, organizational factors and management deficiencies was characterized as an 'apparently insoluble' problem [1].

* Corresponding author. Fax: +1 610 444 6193.
E-mail address: smhess@sensortex.com (S.M. Hess).

0951-8320/$ - see front matter © 2004 Published by Elsevier Ltd.
doi:10.1016/j.ress.2004.10.006

The research described in this paper provides an alternative approach to address this issue. This approach models the impact of nuclear power plant management and processes as a dynamical system. In this approach, plant processes that provide significant impact on nuclear safety risk are identified. Interactions among these processes and plant safety risk are identified and a mathematical model describing the dynamics is formulated. From this model, the impact on plant risk due to the interactions among plant processes are assessed. Insights from this generic model have resulted in a detailed assessment methodology to facilitate plant specific evaluation of the effectiveness of these processes at controlling risk with the capability to provide quantitative data for incorporation into the model.

The approach employed owes much to the initial application of dynamical systems models to diverse problems such as the modeling of insect populations [2], the nuclear arms race and the potential onset of war [3–6]. As for these applications of relatively simple dynamical models to complicated issues, the primary benefit of the dynamical nuclear plant risk model is not in its capacity to provide detailed quantitative estimates of changes in plant risk. The model is significant because it provides a theoretical construct that accounts for the pertinent features of the impact of plant management and processes on commercial nuclear power plant safety risk. As such, its analysis permits the development of insights important to support effective control of risk at these facilities. As will be discussed in this paper, the insights obtained corroborate the results of previous research and the opinion of numerous experts on the importance of management and process factors to plant risk. The conclusions drawn from this analysis also provide quantitative support for the importance of explicit risk management as a cornerstone in ensuring that plant management controls are effective in minimizing nuclear safety risk. Thus, the model and the insights obtained provide useful theoretical support that a transition to a risk-informed, performance based regulatory structure will provide long-term safety benefits and that it can be accomplished without incurring significant public safety impact during the transition.

2. Model development

Operation of a nuclear power plant encompasses many significant interrelated activities performed by numerous individuals. These activities typically are performed using organizations which are compartmentalized with personnel having highly specialized skill sets. Thus, a nuclear power plant has the characteristics of, what Henry Mintzberg has descried as a 'machine bureaucracy [7].' These organizations are distinguished by use of highly formalized and specialized procedures to accomplish operating tasks. They possess formal rules and regulations and communication channels. These organizations also are typified by a relatively centralized decision-making process within an extensive administrative structure [8]. As an example of the degree of complexity involved with management of a modern nuclear power plant, information flow models have been developed to capture the process of conducting maintenance on plant equipment. These models identify 15 separate programs which provide inputs/outputs to the decision-making and execution process [9]. Examples of these programs include the corrective action program, work planning, scheduling, control and execution, equipment/system performance testing and monitoring, preventive maintenance, predictive maintenance, parts procurement, regulatory compliance, etc.

Recently, the industry has developed a multilevel process model which is intended to provide a management tool using three key measures (the process description, cost and performance) to analyze plant performance in a standardized manner [10]. This Standard Nuclear Process Model (SNPM), shown in Fig. 1, has become an industry standard for use in evaluating plant performance. It also is a standard by which operational performance and cost data are collected. Thus, the SNPM provides a useful catalog of plant processes which served as the basic structure from which the dynamical systems model of the impact of these processes and their interactions on plant safety risk was developed.

The SNPM consists of a multilevel process model encompassing all aspects of plant operation. The process is structured to facilitate analysis of plant performance using the key indicators of plant process, cost and performance. The model consists of a multi-level structure which allows collection and analysis of performance data at each level. This structure supports collection of cost and performance data using existing plant information management systems. The structure consists of four levels, with the zeroth level providing a macroscopic view of overall plant operation. At this level, the SNPM consists of the basic structures required to operate a nuclear power plant. Examples include operations, work management, configuration control, equipment reliability, etc.) Each lower level then provides a more detailed view of the individual processes and methods which combine to form the higher level. For example, the work management process is subdivided into several lower level processes including planning, scheduling, preventive maintenance and predictive maintenance.

At the highest level, the SNPM consists of eight basic processes. Of these, five are considered core processes and three are enabling processes. The core processes are those which provide a direct impact on plant operation. They include plant operations, plant configuration control, work management, equipment reliability and materials and services. The enabling processes are those that impact plant performance indirectly, i.e. they are necessary to support the effective and efficient operation of one or more of the core processes. These processes include support services, loss prevention and training. In the SNPM, each

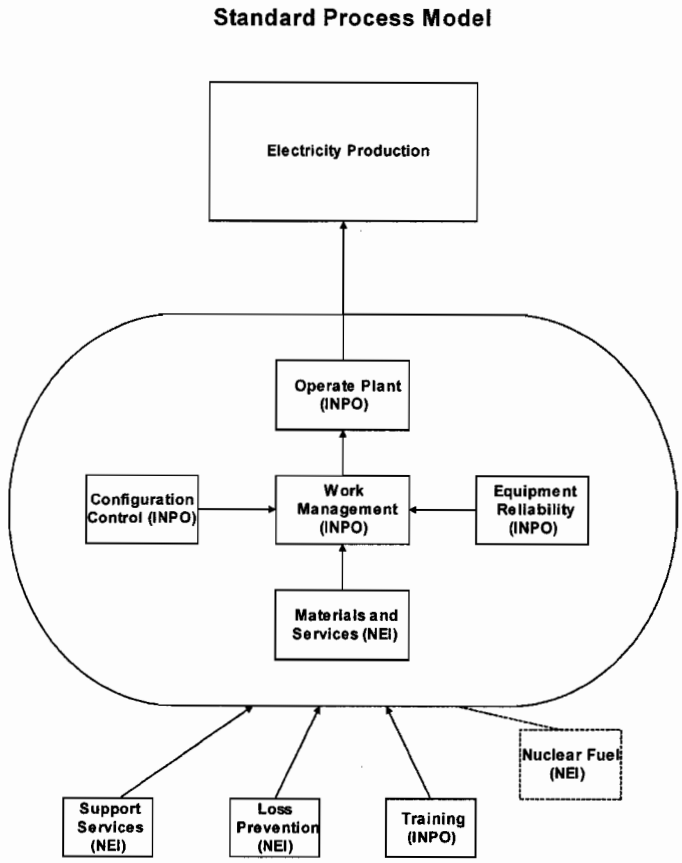

Fig. 1. Nuclear plant standard process model.

process is decomposed into constituent sub-processes required to achieve the objective of the higher-level process. These sub-processes describe the individual functions necessary for the performance of the associated process. The sub-processes also provide the framework from which performance and cost data are obtained and analyzed. In the SNPM, each sub-process is further decomposed into individual activities (second level) and these, in-turn, are decomposed further into individual tasks (third level). These levels correspond to an increasingly microscopic view of the processes. Since the second and third levels are specific to the individual plant's method of conducting business, i.e. they are governed by plant specific procedures and business practices, there is no specific information regarding them in the SNPM.

The first step in developing a dynamical model from which useful plant risk insights can be obtained is the identification of the plant programs which provide a direct and significant contribution to plant risk. Once these parameters are identified, applicable correlations between them must be postulated. In this investigation, only the simplest correlations between different processes were postulated. These limitations were imposed for several reasons. First, although a plethora of data is collected at operating nuclear plants, there are no variables that directly measure the effectiveness of plant programs and processes on plant safety. Thus, development of a complex model could not be supported by field data. Second, development of a simple model permits evaluation both by analytical and numerical methods. It should be noted that this approach has successfully been applied within other contexts, such as cooperative and competing biological systems, to model interactions between different entities [11,12]. Finally, the primary objective of the model is to obtain insights into how plant process interactions and performance impact safety risk. Use of a simple model that reflects actual performance trends, either observed or logically deduced, will best facilitate identification of important insights and conclusions.

Using the SNPM zeroth level processes as representations of the plant and the model constraints discussed above, plant risk can be described as a multidimensional vector consisting of plant risk impact and the performance of the eight core and enabling processes. In development of the model, we define the following variables:

- R, plant risk deviation from the inherent level, (In discussion of this model, we refer to this variable as the

risk performance. It provides an indication of the extent, in terms of relative magnitude and direction, to which the plant risk will deviate from that estimated in the PRA due to the performance of the other modeled plant processes. In the context of risk management, this is the primary variable in which we are interested)

- O, plant operational performance,
- C, plant configuration control performance,
- W, work management process performance,
- M, materials and services process performance,
- E, equipment reliability process performance,
- S, support services process performance,
- L, loss prevention process performance,
- T, plant training performance.

Note that all US nuclear power plants have detailed PRA's for most potential initiators that can lead to reactor core damage. Core damage frequency (CDF) provides the commonly accepted surrogate measure of public safety. These PRA's use mean frequencies and event probabilities to estimate this inherent level of risk.

Thus, the plant risk dynamics due to plant programs and processes are potentially represented by a nine dimensional vector

$$\mathbf{X} = (R, O, C, W, M, E, S, L, T). \tag{1}$$

In this model, the performance of the individual processes is defined over the range $-1 \leq X_i \leq 1$ where X_i represents the i-th constituent variable. In this scheme, a negative value of X corresponds to ineffective performance, a positive value to effective performance. The result $X=0$ represents a point where the program neither improves nor hinders plant safety; i.e. the point of indifferent performance. Specifically, for the risk performance variable, $R<0$ indicates poor risk performance and thus indicates an increase in overall plant risk from the baseline estimated in the PRA. $R>0$ indicates effective risk performance and thus indicates a decrease in overall plant risk. Limiting the range of the constituent variables was chosen for two reasons. First, as discussed above, the model possesses only a qualitative relationship to the plant risk as estimated in the PRA. Thus, results obtained are not intended to be used to 'update' these quantitative results. Second, there are physical (i.e. economic and regulatory) constraints on process performance; i.e. it cannot run away to infinity. This is accomplished by limiting the range of the process performance; i.e. if in any iteration step $|X_i|>1$, then, by definition, the variable is set to ± 1 as appropriate.

Given the model constraints discussed above, the most general evolution of any component at future time $t+1$ is related to the parameters at present time t by

$$X_i(t+1) = \sum_i \lambda_i X_i(t) + \sum_{i,j} \mu_{ij} X_i(t) X_j(t) + \kappa_i X_i(t)^3. \tag{2}$$

The first term on the right hand side is simply the linear component of the relationship, the second term represents the quadratic couplings including programmatic interdependencies and the third a possible cubic in the variable itself. Note that in this model, time (t) is a discrete variable. Modeling the dynamical plant risk performance as a map was chosen to correspond to the incidence of data collection for management purposes at these facilities. Since this type of data typically is obtained on a monthly basis, the discrete time interval in the model also is taken to be monthly. This choice will permit future acquisition and analysis of field data. It should be noted that, at this point, the impact of plant risk culture is not included.

We have developed a version of the dynamical risk model that incorporates the impact of plant risk culture. This revision to the model resulted in several significant insights into the important benefical effects of a strong safety culture (and deleterious effects of a poor one). However, this revision to the model is significant and thus, its basis and the effects of its inclusion in the model will be described in a subsequent paper.

In application of the model to operational plants, the estimation of the interprocess coupling parameters is anticipated to be a difficult activity. These parameters currently are not measured in any meaningful sense at commercially operating plants. Additionally, since they are somewhat subjective, one can anticipate large uncertainties in their estimates. Since plant programs are designed to work cooperatively to achieve common objectives, each coupling parameter is postulated to have a value that is positive or zero, with a coupling parameter ~ 1 indicating a fairly strong coupling. Thus, it is anticipated that the actual estimates for these parameters will fall in the range [0,1] in cases representative of commercially operating plants. Within this framework, it is suggested the parameters can be estimated from the following characteristics provided in Tables 1 and 2 for the linear and quadratic couplings, respectively.

As will be discussed later in the section in which the techniques of dynamical systems theory are used to analyze the model, only large values of λ and μ lead to chaotic dynamics. Since for most operating nuclear plants, these values are expected to be ~ 1 or less, system response, in a qualitative sense, is not expected to be affected significantly by the errors inherent in the parameter estimates. Thus, the classification provided above will be sufficient to characterize the dynamics and obtain useful insights.

To develop a model which can provide useful insights to plant risk, the next task is to identify the most significant interactions. To accomplish this each program was analyzed to eliminate those interactions which are not expected to provide a substantial effect. Additionally, several of the processes as defined in the SNPM are mutually supporting, and from a plant safety viewpoint, can be combined within the model. This analysis is summarized below.

Table 1
Linear coupling values

λ_{jk}	Description
0	No discernable impact from process j on process k
~0.01	Process j provides minimal input but results rarely impact process k
~0.05	Process j provides minor input with occasional impact on process k
~0.1	Process j provides input which impacts process k relatively frequently
~0.25	Process j provides frequent input which often impacts process k
~0.5	Process j provides input which nearly always impacts process k significantly
~1	Process j provides continual input which nearly always impacts process k significantly
~2–5	Process j provides continual input which serves to direct decisions made in process k

Training on safety culture? Who trains you to do more than what's required?

Not included.

3. Analysis of SNPM processes and interactions

3.1. Training

In nuclear power plants, programs to train various plant personnel, particularly operations, maintenance and engineering personnel, are strictly controlled as to both the content and methods used. For example, all training modules have formal lesson plans with student learning objectives and example test questions. Additionally, implementation of many activities requires demonstrated on-the-job skill proficiency with sign-off of qualification standards by experienced instructors and/or supervisors in the responsible discipline. Finally, these training programs are reviewed and accredited on an ongoing basis by external agencies. Thus, any deficiencies or degraded performance are routinely identified. Because of these limitations, the effectiveness of the plant training programs is expected to vary only very slowly over time and over a very narrow range. Thus, from a dynamical viewpoint, the effectiveness of the training program at time $t+1$ can be assumed to be the same as that at time t. Therefore, although training has an important impact on plant safety, its impact is relatively constant over time. Because of this characteristic, this program will have negligible impact on the change in plant risk when compared to the performance of other plant programs. Hence, the performance of the training program is not included as a variable in the dynamical risk model.

3.2. Support services

The support services process provides support to the core SNPM processes. The impact of this process on plant safety is indirect through its impact on the core processes. Additionally, for those functions necessary to support the core processes, contingency methods are available to perform these functions in the event of failure of one of the support services processes. As an example, all plants possess manual methods and procedures to process necessary work orders (i.e. support the work management core process) in the event the electronic system is not operating (i.e. failure of the function to provide information technology services). Thus, from the viewpoint of plant safety, this process does not provide a significant impact and can be ignored in the model.

3.3. Configuration control

The plant configuration control process, that is maintaining the plant engineering design basis within prescribed technically acceptable limits, consists of two parts. The subprocess 'provide configuration control' is an ongoing daily function conducted as part of the responsibility of plant operations to control various plant evolutions. The remaining sub-functions all address issues which can impact plant safety in the long term. However, each of these functions does not vary appreciably over the short term. Thus, the subprocesses that dynamically impact risk can be incorporated within the performance of the operations process; hence eliminating this as an independent variable.

3.4. Operations

Plant operations provide a direct and immediate impact on plant safety. Operations personnel provide the primary line of defense to respond to plant transient and accident

Table 2
Quadratic coupling values

μ_{jk}	Description
0	No discernable collaboration between process j with process k in k's decision-making process
~0.01	Minimal collaboration between process j with process k in k's decision-making process
~0.1	Occasional collaboration between process j with process k in k's decision-making process
~0.25	Frequent collaboration between process j with process k in k's decision-making process
~0.5	Significant collaboration between process j with process k in k's decision-making process
~1	Continual collaboration between process j with process k in k's decision-making process
~2–5	There is constant collaboration between process j with process k in k's decision-making process; and decisions are nearly always achieved by some degree of consensus

situations. Conversely, operational errors, either of commission or omission, can result in events that initiate or contribute to plant conditions that increase risk. In this function, the plant operators identify and diagnose the condition of the plant, confirm that appropriate automatic designed safety actions occur and, if they do not, they manually implement them. Additionally, plant operations are conducted in a high-pressure environment. Due to the large financial consequences associated with lost power production, this level of pressure is manifest during normal operations. During transient or accident conditions, it is greatly magnified. In addition, operational performance depends to a great extent on the effectiveness of other interfacing plant processes. As a primary example, operational effectiveness directly depends on the effectiveness of the plant work management program to correct identified deficiencies in a timely manner. Poor maintenance typically results in poor availability and reliability of installed plant equipment. If this occurs, the resulting poor equipment performance can reduce the ability of plant operators to adequately perform necessary activities. Additionally, a legacy of maintenance problems can lead to operators not believing various indications that a situation is deteriorating, resulting in delays in implementing appropriate actions or in implementing actions which are deleterious to the situation encountered.

The performance of the equipment reliability process primarily is manifested to operations via its impact on the plant work management program, in particular in its impact on plant maintenance. For example, issues such as analyzing equipment performance data and performing troubleshooting of plant problems are manifest, from an operational perspective, in the ability to effectively and efficiently schedule appropriate equipment maintenance activities. Thus, operational performance also is postulated to be independent of the current equipment reliability program performance. Finally, since the loss prevention process addresses the root cause and performance enhancement functions, operational performance will be somewhat dependent upon this process. However, since loss prevention typically addresses longer-term issues, the dependence is expected to be much weaker than for the dependence on the work management process. Based on this discussion, future operational performance is postulated only to depend upon the current performance level of the operational and work management functions, i.e.

$$O(t+1) = f(O(t), W(t)). \tag{3}$$

In nuclear power plants, progression through positions of increasing responsibility in the operational staff requires a combination of training and job experience. Since it requires a significant amount of time for personnel to achieve these requirements, future operational performance should be a slowly varying function of current operational performance. Thus, ignoring the interaction with other processes (such as work management), we expect $O(t+1)=O(t)$. As stated previously, maintenance performance does have a direct impact on operational performance, i.e. effective maintenance improves operational performance. Additionally, operations and maintenance interact daily to identify and resolve equipment problems; hence, there is a significant interdependence between these variables. Thus, the operations performance at the next time interval $t+1$ can be modeled to be the sum of the current operational performance and coupling terms dependent upon the current performance of the work management and loss prevention functions and a term representing the degree of collaborative interaction between the operations and work management processes. Defining the coupling parameter for the direct influence of the work management processes on operations as λ_{WO} and the operations–work management collaborative interaction term as μ_{MO}, we obtain the dynamical equation for operational performance

$$O(t+1) = O(t) + \lambda_{WO}W(t) + \mu_{WO}W(t)O(t). \tag{4}$$

Note that if the coupling terms are small, then operational performance will be relatively constant, in agreement with our previous discussion. However, if the coupling is large, then the performance of the operations and work management processes become highly interdependent. In plants with excellent operational performance that are recognized as industry leaders, there is evidence that a high degree of interdependence between these functions occurs and that significant safety benefits are realized [13].

3.5. Materials and services process

Of the eight materials and services sub-processes, five directly support the work management core process (i.e. plant maintenance). Thus, from a nuclear safety viewpoint, they can be combined with the work management process. The sub-process to provide disposal and surplussing provides an economic function for the plant with minimal impact on plant safety. The final two sub-processes of providing and transporting fuel and providing handling, storage and disposal of fuel have nuclear safety impact; however, they are independent of the primary function of generating electricity and are not typically considered as normal plant operational functions nor are they modeled as part of the plant PRA. Additionally, these activities have independent stand-alone regulatory requirements and procedural controls. Thus, these subprocesses are not included within the framework of the dynamical systems risk model.

3.6. Work management process

Along with plant operations, execution of plant maintenance provides a direct daily impact on plant safety. Plant maintenance performance is regulated under provisions of the maintenance rule [14] with implementation primarily performed by the plant engineering

organization. However, being the first example of a risk-informed, performance-based regulation, regulatory scrutiny focuses upon monitoring performance of plant systems, structures and components (SSC's). Thus, many of the actions required by the maintenance rule are performed as part of the equipment reliability and loss prevention processes.

Similar to the case of operational performance, the current level of plant safety, as manifested in the CDF, has a negligible impact on the effectiveness of the maintenance program. But maintenance program performance is intimately coupled to the performance of the operations and equipment reliability processes. First, the work management program relies upon the effectiveness of operations to identify failed or degraded components through normal operational activities and plant operational surveillance testing. It also relies on appropriate work prioritization and scheduling. The conduct of maintenance requires operational support for equipment removal and return to service. Finally, operational support is required for post-maintenance acceptance testing. Likewise, the conduct of the maintenance program is dependent upon the effectiveness of the equipment reliability program. This includes equipment and system performance monitoring for identification of degraded performance, appropriate work prioritization and efficient planning and scheduling. This also includes an analysis of the risk to plant safety and, for conditions which require addition of a significant level of risk, development of appropriate controls and contingency actions to mitigate these factors. Finally, since the loss prevention process addresses the root cause and performance enhancement functions, operational performance will be somewhat dependent upon this process. However, since loss prevention typically addresses longer-term issues, the dependence is expected to be weaker than for the previous cases.

Based on this analysis, we define the coupling parameters between the work management program performance and operational, equipment reliability and loss prevention program performance to be λ_{OW}, λ_{EW} and λ_{LW}, respectively. We similarly define the work management–operations and work management–equipment reliability interaction terms to be μ_{OM} and μ_{EM}, respectively. We thus obtain for the evolution of the work management process performance

$$W(t+1) = W(t) + \lambda_{OW}O(t) + \lambda_{EW}E(t) + \lambda_{LW}L(t) + \mu_{OW}O(t)W(t) + \mu_{EW}E(t)W(t). \quad (5)$$

Again, note that if the coupling terms are small, then work management process performance will be relatively constant. Additionally, it should be noted that the linear coupling terms between operations and work management are not necessarily equal, i.e. $\lambda_{OW} \neq \lambda_{WO}$ in general. For example, it is quite possible that one process may be much stronger in its influence on the other than vice versa. However, since the quadratic coupling is indicative of collaborative interaction, it generally can be postulated that these terms will be roughly equal, i.e. $\mu_{OW} \approx \mu_{WO} \approx \mu$.

3.7. Equipment reliability process

In the SNPM, the equipment reliability function focuses on the programmatic aspects of ensuring that plant structures, systems and components are maintained at high levels of reliability and availability. Ensuring this equipment reliability is a function of the engineering organization. The effectiveness of this activity is highlighted by implementation of the maintenance rule [14] which requires monitoring of the performance of plant SSC's. One result of this rule is that SSC's with identified performance deficiencies are required to have performance improvement programs developed with increased senior management oversight of the specified corrective actions, including monitoring of their effectiveness. Other aspects of plant engineering that impact equipment reliability include preventive and predictive maintenance programs, system health monitoring activities, and performance monitoring and improvement initiatives. These programs provide stringent controls on plant equipment performance. Additionally, these plant programs are evaluated on a continuing basis both by industry peer organizations and regulatory bodies; i.e. INPO and NRC.

A consequence of these aspects of the equipment reliability function is that it is predominantly self-sufficient. If process effectiveness degrades, there are strong pressures to improve performance and return it to an acceptable level. As an example, if a plant experiences repetitive equipment failures that result in plant trips or excessive safety system unavailability, significant emphasis on identifying and correcting the root causes of these failures will be expended. Typically, this improvement effort will be initiated by the licensee due to the potential economic impact of these events. However, if these efforts do not correct the problem or if the events experienced are significant, the regulatory authority will become involved and require a more extensive and comprehensive response. Additionally, the regulatory approach and economic incentives are structured such that the further degraded the performance, the more severe the regulatory impositions, including the possibility of imposing a plant shutdown with concomitant severe economic consequences for the owner. Thus, degraded process effectiveness will result in senior management attention and application of additional resources to address its basic causes. As a general principle, the further the performance is from acceptable, the more resources will be applied to improve it. Conversely, there are strong economic constraints which limit the level of effectiveness which can be maintained in practice. As a business enterprise with the economic objective of maximizing profits, nuclear plants have access to significant, but not unlimited, resources. Personnel and technologies utilized to ensure equipment

more of a problem
more resources

reliability are specialized and expensive. Thus, there is a strong economic constraint to maintain equipment reliability at a sufficiently high level, i.e. one which meets identified requirements such as the maintenance rule performance criteria, but to not apply the large marginal expenditures necessary to further improve performance.

In the initial modeling of the equipment reliability process, these limitations are accounted for via use of a cubic function. Defining $E \equiv 0$ as the operating point of indifferent performance; i.e. the point at which performance neither improves nor degrades safety, the function

$$E(t+1) = (E(t))^3 \tag{6}$$

can be used to represent the performance of the equipment reliability process. Notice that this representation of performance is stable about this operating point, i.e. $E=0$ is a fixed point and $|dE/dt| < 1$ [15]. Also notice that this model has the characteristic that as one moves further in either direction from the fixed point, the economic forces increase to return it to that point.

Mathematically, a pure cubic function results in a very rapid attraction to the stable fixed point $E=0$. However, due to the specialized nature of the resources that perform this function and its complex nature, its performance is not expected to change very quickly. Thus, the behavior obtained via a pure cubic model is not realistic. Modification of the model to include a linear term will result in a more gradual change in performance. Requiring the range of E to be the interval $[-1, 1]$, we obtain

$$E(t+1) = a_1 E(t) + a_2 E(t)^3 \tag{7}$$

with the constraint $a_1 + a_2 = 1$. Note that the more dominant the linear term, $a_1 > a_2$, the more slowly performance moves to the point of indifference ($E=0$). Also note that constant performance at any point $E \neq 0$ can be obtained by setting $a_1 = 1$, $a_2 = 0$.

3.8. Loss prevention process

The loss prevention function includes providing security, safety, fire protection and emergency planning. It also includes performance monitoring and improvement including the plant PRA (and staff responsible for the PRA). The loss prevention function has many of the same characteristics as the equipment reliability function. Each of the constituent sub-processes provides support to maintaining plant safety, either directly or in concert with plant performance improvement initiatives. In contrast to the equipment reliability process, the functions associated with the loss prevention process each have the attribute that they are performed off-line; i.e. they typically do not need to be inserted directly into the core processes on a daily basis. However, these processes are necessary to ensure that plant safety and performance are maintained over the long term. Normally, these functions are the responsibility of the plant engineering organization. Of paramount importance for nuclear safety is the function to provide performance monitoring and improvement services. This function includes all aspects of event and performance analysis including self-assessment, root cause determination, corrective action specification and effectiveness monitoring, human factors performance and analysis, regulatory compliance, supplier qualification and plant quality assurance.

Similar to the equipment reliability function, loss prevention has the characteristic of possessing strong economic and regulatory imperatives which tend to drive performance to a point of indifference over time. If the effectiveness of the function decreases, there are strong regulatory pressures to improve performance and return it to an acceptable level. Similarly, there are strong economic constraints which limit the level of effectiveness which can be maintained in practice. Thus, the loss prevention function can be characterized by the same model as used for the equipment reliability function. Thus,

$$L(t+1) = b_1 L(t) + b_2 L(t)^3 \tag{8}$$

with the similar constraint $b_1 + b_2 = 1$.

3.9. Plant risk

While not producing a significant influence on the performance of the analyzed SNPM process performance levels, the existing level of plant risk is directly related to the performance of these programs. However, this dependence is an inverse relationship. As performance in any of the plant programs improves, the overall plant risk will decrease. However, in the proposed model, we defined R as the plant risk performance which is indicative of the deviation from the baseline value of risk due to the performance of the various processes included in the SNPM. With this definition of R, the relationship between R and the other model parameters is direct.

Since there are no a priori known interrelationships between plant risk and performance of the SNPM programs, the simplest relationship is proposed, i.e. a linear one. Note, however, that because the dynamical performance of the various plant programs on which plant risk depends are nonlinear, this choice still results in a nonlinear model. Defining the coupling parameters between plant risk performance and the operations, work management, equipment reliability and loss prevention process effectiveness as α_O, α_M, α_E and α_L, respectively, with each $\alpha_i \geq 0$. We have the general equation for plant risk performance at time $t+1$.

$$R(t+1) = \alpha_O O(t) + \alpha_W W(t) + \alpha_E E(t) + \alpha_L L(t). \tag{9}$$

Notice that in this model, if all process performances are indifferent, then the risk performance also operates at

the level of indifferent performance, i.e. $R=0$. Recall that in this model we defined R as the degree to which plant risk deviates from the level inherent in the design. Thus, if the plant is operating at the level of indifferent risk performance; the actual plant risk is at its natural level based on the physical design. Thus, operation at a level such that $R=0$ corresponds to the value of CDF estimated in the PRA with R providing a relative indicator of the risk deviation from this level. Note that due to this definition, the model result cannot be converted directly into a calculated change in the CDF. However, the model does provide a relative indicator of the change in risk that provides both a direction (i.e. increase or decrease) and relative magnitude. From this model, an assessment methodology was developed which provides a plant specific evaluation of the performance of these processes. This assessment process provides valuable information to plant operators to monitor the effectiveness at which the plant processes are controlling risk [16,17].

As discussed in the previous sections, operations and maintenance have a direct and immediate impact on plant safety. Thus, in general, we expect the maintenance and operational coupling to be comparable, $\alpha_W \sim \alpha_O$. Additionally, since risk is directly coupled to the operations and work management processes, if these processes individually are made perfectly effective, then plant response to any external initiating event will always be as designed and $R \to 1$, i.e. the undesired event will never occur. Conversely, if they individually are made totally ineffective, risk will increase to a maximum level and $R \to -1$, i.e. the undesired event becomes certain. Thus, we set $\alpha_O = \alpha_W = 1$ in (9). Additionally, we postulate that the risk mitigation functions of equipment reliability and loss prevention impact plant risk only through their effects on the operations and work management processes. Thus, we can set the interaction parameters $\alpha_E = \alpha_L = 0$ and the model for the risk performance reduces to

$$R(t+1) = O(t) + W(t). \tag{10}$$

In summary, the dynamical risk model can be characterized by the system of finite difference equations

$$\begin{aligned} R(t+1) &= O(t) + W(t), \\ O(t+1) &= O(t) + \lambda_{WO} W(t) + \mu_{WO} W(t) O(t), \\ W(t+1) &= W(t) + \lambda_{OW} O(t) + \lambda_{EW} E(t) + \lambda_{LW} L(t) \\ &\quad + \mu_{OW} O(t) W(t) + \mu_{EW} E(t) W(t), \\ E(t+1) &= a_1 E(t) + a_2 E(t)^3, \\ L(t+1) &= b_1 L(t) + b_2 L(t)^3. \end{aligned} \tag{11}$$

This model accounts for the important process interactions that impact plant risk, including those that specifically are designed to mitigate risk (i.e. equipment reliability and loss prevention). However, this model does not account for the impact of the plant 'risk culture'. In a future paper we will discuss how the model can be modified to account for this characteristic and demonstrate how a strong risk culture provides important safety benefits.

Link to Safety Culture

4. Prliminary model analysis

In this section we provide some results and insights from analysis of the system described by (11) using simple analytical methods. More detailed results obtained from numerical simulations will be reported in a separate paper.

Understanding the behavior of dynamical systems is predicated upon the identification of the equilibrium points for the system and characterizing their stability with respect to perturbations. For a map of the form

$$\mathbf{x}(k+1) = \mathbf{f}(\mathbf{x}(k)) \tag{12}$$

the fixed points are those where the value of the variable does not change, i.e. the points $\mathbf{x}^*$ where

$$\mathbf{x}(k+1) = \mathbf{x}(k) \equiv \mathbf{x}^*. \tag{13}$$

For systems described by multiple variables, such as (11), evaluation of the stability of the fixed points requires evaluation of how each variable responds to changes in each of the others. This is obtained by evaluation of the Jacobian matrix at the fixed points. Let $\mathbf{f}(k)$ be an n-dimensional map with $\mathbf{f} = (f_1, f_2, \ldots, f_n)$ with each f_i a function of the n variables $x_j(k)$ ($f_i(k) = f_i(x_1(k), x_2(k), \ldots, x_n(k))$ for $i = 1, 2, \ldots, n$; $k = 1, 2, \ldots$). Also let $\mathbf{x}^*$ be a fixed point of the system where we note $\mathbf{x}^*$ is an n-component vector obtained from the solution of

$$\mathbf{x}^*(k+1) = \mathbf{f}(\mathbf{x}^*(k)) \tag{14}$$

To obtain the stability of the point $\mathbf{x}^*$, let $f_i^j = \partial f_i / \partial x_j$ be the partial derivative of f_i with respect to variable x_j. Then, the Jacobian consists of the matrix with ij-th component f_i^j evaluated at the fixed point $\mathbf{x}^*$, i.e.

$$[\mathbf{D}f(\mathbf{x}^*)]_{ij} = (\partial f_i / \partial x_j)|_{\mathbf{x}^*}. \tag{15}$$

Applying a generalized Taylor expansion of $\mathbf{f}$ about the fixed point $\mathbf{x}^*$, we have for a small vector $\mathbf{h}$

$$\mathbf{f}(\mathbf{x}^* + \mathbf{h}) - \mathbf{f}(\mathbf{x}^*) \approx \mathbf{D}f(\mathbf{x}^*) \cdot \mathbf{h}. \tag{16}$$

The stability of the fixed point is obtained from the magnitudes of the eigenvalues of the characteristic equation of $\mathbf{Df}(\mathbf{x}^*)$. Recall the eignevalues are determined by the characteristic equation obtained from the determinant

$$\det(\mathbf{D}f(\mathbf{x}^*) - \lambda \mathbf{I}) = 0 \tag{17}$$

where λ are the eigenvalues and $\mathbf{I}$ is the identity matrix. Then, for a map, $\mathbf{x}^*$ is a sink if the magnitude of each eigenvalue of $\mathbf{Df}(\mathbf{x}^*) < 1$. Conversely, if the magnitude of each eigenvalue of $\mathbf{Df}(\mathbf{x}^*) > 1$, then $\mathbf{x}^*$ is a source. Notice that for a fixed point to be locally stable, it is

required to be stable in the direction of each eigenvector [15].

4.1. Equipment reliability and loss prevention functions

Because the dynamics of the equipment reliability (E) and loss prevention (L) functions are self-contained, each can be evaluated by simple one-dimensional analysis. The equations are of the same form and each possess three fixed points at 0 and ± 1. Additionally, because these functions are governed by one-dimensional finite difference equations, the stability criterion of the Jacobian determinant reduces to a simple ordinary derivative. Analysis of the stability of these fixed points demonstrates that $E(L)=0$ is a sink and the points at $E(L)=\pm 1$ are sources. Thus, this function possesses the characteristic that performance will tend to the point of indifferent effectiveness. This characteristic has been qualitatively observed at commercial nuclear plants. This is due to the following reasons. First, the application of highly skilled resources is required to achieve an effective level of performance. Since these resources are expensive to obtain and retain, there exist strong economic pressures to limit their application. As described previously, if performance of either of these functions is poor, there will be significant pressure supplied by both plant management and the regulator to improve performance to a level that is deemed to be acceptable. In an operational plant, poor performance can be manifest in numerous ways such as repeat equipment failures, high levels of plant trips or safety system unavailability, etc. Within the context of the dynamical risk model, this is equivalent to performance values $X_i<0$. Pressure to improve performance can take numerous forms, including in extreme cases, forced shutdown of the plant. This capability of the regulator provides a countervailing incentive to limit the extent to which resources can be drained away from these functions. The combined action of these forces results in their performance trending, over time, to a level of indifferent effectiveness with only small variations about this level.

An important question that arises with respect to these risk mitigating functions is how their coefficients can be estimated. Typically, both the equipment reliability and loss prevention functions at commercial nuclear plants are performed by engineering professionals. These personnel typically have an understanding of engineering fundamentals and specific training in their respective roles within the plant. The effectiveness with which these personnel perform these functions is, to a large extent, a matter of both formal knowledge and experience. Thus, a major factor in determining the time frame in which performance would return to the point of indifference, i.e. neither improving nor hindering plant safety, is the time frame in which the plant engineering organization personnel turnover and used of the turnover rate of engineering resources can be used to provide an estimate for the coefficients in the loss prevention and equipment reliability functions. Plants that experience high personnel turnover in these key functions can be postulated to correlate with lower performance levels than for plants with lower turnover. This is due predominantly to the greater average level of experience, both in terms of general nuclear plant knowledge and technology specific expertise, of personnel in the low turnover case.

turnovers

Recall that the model for these processes contains both a linear and a cubic term over the interval $[-1, 1]$

$$X(t+1) = aX(t) + bX(t)^3 \tag{18}$$

where X represents either E or L. To maintain X in the range $[-1, 1]$, we have the constraint given by $a+b=1$. Note that the more dominant the linear term ($a>b$), the more slowly performance moves to the point of indifference ($X\equiv 0$). Therefore, in this model, as plant engineering staff turnover increases, the linear term (a) can be expected to decrease with the cubic term (b) correspondingly increasing. Using this model for either the equipment reliability or loss prevention function, the time to return to the point of indifferent performance was calculated for various values of the linear coefficient (a) and initial value of process performance. Results are shown in Fig. 2. In this figure, each curve represents a given initial performance level, with values of the initial condition set equal to 0.1, 0.2, 0.4, 0.6 and 0.8 displayed in the figure. Each curve shows the calculated time to return to a level of indifferent performance as a function of the linear coefficient (a) in (18). Notice that these curves all possess the same shape and are closely spaced. This indicates this model will be applicable to any operating commercial nuclear plant regardless of the current level of performance of these functions. However, one should be aware that this function also can change abruptly if the system is subject to a severe external shock such as a regulatory imposed shutdown, change of ownership, etc.

what causes a to increase?

As expected, rapid staff turnover, which is exhibited by a smaller linear coefficient in the model equations, will result in a fast decrease in the effectiveness of the respective risk mitigating process. Conversely, if the staff remains stable, resulting in a larger linear coefficient, the program can remain effective and provide positive safety benefits for relatively long periods of time. From Fig. 2, the model indicates a decrease in performance to the indifferent level occurring in a time frame ~ 2 years corresponds to a linear coefficient of 0.6–0.7. One method for this to occur would be a complete turnover in the staff that performs these functions. Thus, the model indicates that staff turnover rate can serve as a conservative surrogate measure of the linear coefficient. In applications at commercial facilities, the minimal expected values of the linear terms should be in the range of 0.5–0.6 (corresponding to a less than 2 year turnover rate), with significantly higher values for plants with more stable staffs. Due to the significant training

large turnover, months for change very short,

low turnover, long time for change

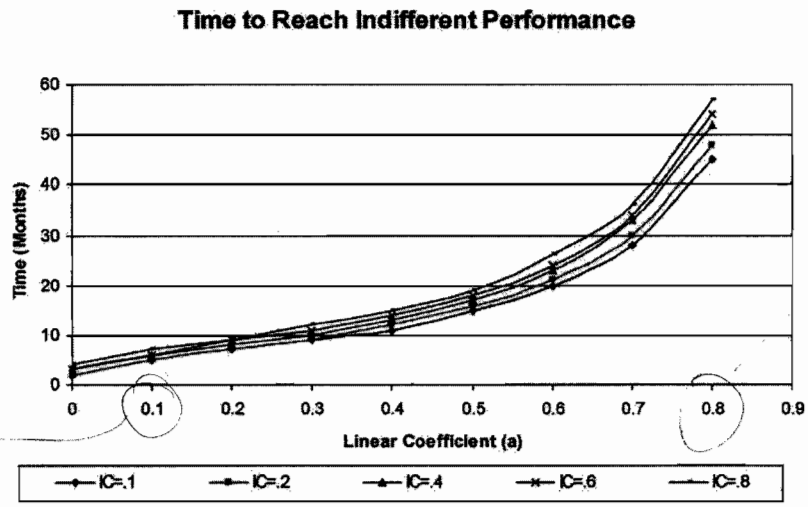

Fig. 2. Plot of time to reach indifferent performance vs. linear coefficient for equipment reliability and loss prevention functions. IC, initial condition for process performance.

provided to plant personnel that perform these functions, a 2 year staff turnover represents a reasonable lower bound in estimating the linear coefficient for the equipment reliability function. Additionally, since the constituent parts of the loss prevention function are more specialized, they typically are staffed with more experienced personnel than for the equipment reliability function which is the responsibility of station system engineering personnel. Thus, the loss prevention function typically will be expected to have a smaller cubic coefficient and a correspondingly larger linear term than the equipment reliability function.

4.2. Analysis of simplified ROW model

An important aspect of the dynamical risk model is the importance of the nonlinear interaction terms. As described in Section 4.1, an important simplification can be achieved by setting the risk mitigating equipment reliability and loss prevention functions to their stable point of indifferent operation, i.e. $E=L=0$. This reduces the model to a simpler map on $\mathcal{R}^3$ from which we obtain the following simplified model (which we designate the ROW model)

$$\begin{aligned} R(t+1) &= O(t) + W(t), \\ O(t+1) &= O(t) + \lambda_{WO}W(t) + \mu_{WO}W(t)O(t), \\ W(t+1) &= W(t) + \lambda_{OW}O(t) + \mu_{OW}O(t)W(t). \end{aligned} \tag{19}$$

This simplified model is important for the following reasons. First, because it operates in a three dimensional state space, its evolution is easy to visualize and its dynamics are readily analyzed via analytical (vs. numerical) methods. Second, the assumption that plant risk is dependent upon only the operations and work management processes corresponds to applications where the specific risk management processes of equipment reliability and loss prevention are either not present or are insufficiently developed to be effective. Since this state of affairs is typical of many unregulated process industries, the simplified model possesses great generic applicability. Finally, even this simple model produces rich dynamics in which unstable operating regimes can occur; thus producing regions were programmatic deficiencies can contribute to conditions conducive to increased risk [18].

Similar to the analysis for the E and L functions, we obtain the fixed points for the ROW model from the system of algebraic equations

$$\begin{aligned} R^* &= O^* + W^*, \\ O^* &= O^* + \lambda_{WO}W^* + \mu_{WO}W^*O^*, \\ W^* &= W^* + \lambda_{OW}O^* + \mu_{OW}O^*W^* \end{aligned} \tag{20}$$

By inspection, the origin is a fixed point solution to this system. This result can be interpreted to indicate that if the operations and work management processes function at a point of indifferent performance (i.e. they neither improve nor degrade risk), then plant risk will not deviate from the inherent level due to the plant design. This also can be interpreted to indicate that for indifferent levels of performance of these programs, a PRA will provide an accurate estimate of plant risk. An additional solution to (20) obtains a fixed point at

$$\begin{aligned} (R^*, O^*, W^*) = &(-(\lambda_{WO}\mu_{OW} + \lambda_{OW}\mu_{WO})/\mu_{WO}\mu_{OW}, \\ &- \lambda_{WO}/\mu_{WO}, -\lambda_{OW}/\mu_{OW}). \end{aligned} \tag{21}$$

This fixed point lies in the negative octant of the $\{R,O,W\}$ phase space. Note that operation at this fixed point is indicative of a higher level of plant risk than that inherent in the design and estimated in a PRA.

We next look at the stability of these points. Application of the Jacobian determinant to the fixed point at the origin obtains eigenvalues $\lambda = \{0, 1-(\lambda_{WO}\lambda_{OW})^{1/2}, 1+(\lambda_{WO}\lambda_{OW})^{1/2}\}$. For this case, all of the eigenvalues are real. However, the eigenvalue $1+(\lambda_{WO}\lambda_{OW})^{1/2}$ has magnitude greater than one. Since not all of the eigenvalues are within the unit circle, the fixed point $\mathcal{R}^* = (0,0,0)$ is unstable. Additionally, since none of the eigenvalues is equal to one, the origin is a saddle point. The fact that the origin is not a stable fixed point is not unexpected. In practice, routine operational and maintenance activities constantly alter the risk profile of the plant. Thus, it is not expected that the plant will remain at its level of inherent design risk.

Next, we apply this technique to the other fixed point of the system. For this case the eigenvalues are found to be $\lambda = \{0, 1-\lambda_{OW}\mu_{WO}/\mu_{OW}, 1-\lambda_{WO}\mu_{OW}/\mu_{WO}\}$. All of these eigenvalues also are real. Additionally, since all of the parameters are positive, for values of the λ's not too large (in most instances we expect $\mu_{OW}/\mu_{WO} \approx 1$), all of the eigenvalues will have magnitude less than one. Thus, this point represents a stable fixed point of the system. Because this fixed point is stable, the simplified ROW model indicates that plant risk will tend to this point. Because the value of the plant risk component at this fixed point is negative, this indicates a level of risk greater than the inherent level and agrees with results reported by other researchers via qualitative analyses [19,20].

However, this additional level of risk can be reduced by explicit management focus on the operations and work management decision-making processes. This can be seen by looking at the following simplification of the ROW model. Assume that the linear interaction parameters between operations and work management are equal, i.e. set $\lambda_{WO} = \lambda_{OW} \equiv \lambda$. We similarly assume that the quadratic interaction parameters between operations and work management also are equal, i.e. $\mu_{WO} = \mu_{OW} \equiv \mu$. Then, the value of the stable fixed point reduces to

$$\mathcal{R}^* = (-2\lambda/\mu, -\lambda/\mu, -\lambda/\mu). \tag{22}$$

Inspection of this stable fixed point indicates one way that risk can be minimized is by minimizing the ratio λ/μ. Programmatically, this minimization is equivalent to maximizing the collaboration and interaction between operations and the organizations involved in the work management processes. This conclusion provides a useful prescription for minimizing safety risk. It also qualitatively corroborates experience obtained from accident investigations from many different process industries. For example, recall the previous identification of the importance of poor communications as a contributing factor in industrial accidents. Thus, an important component of risk management at nuclear power plants is to focus resources and management attention on achieving open and effective communications, both within and between the different plant organizations in their respective decision-making processes.

5. Conclusions

In this paper, we have provided some initial results of research conducted to develop a dynamical systems model to assess the impact of plant process performance on nuclear power plant safety risk. The model developed constitutes a five dimensional system of finite difference equations involving the variables of risk and performance of the plant operation, work management, equipment reliability, and loss prevention processes over a normalized domain space and was based on the Standard Nuclear Plant Process model which has found widespread acceptance in the United States as a tool to obtain plant economic and performance data. Simple analysis of the model was demonstrated to provide results that corroborated the opinions of previous researchers on the potential impact of plant management and processes on nuclear safety risk. In addition, some insights into the underlying dynamical causes of these impacts and relevant management strategies to mitigate their impact were identified.

The model was developed using an accepted economic process model applied throughout the US nuclear industry. Thus, the model directly corresponds to processes that exist in all commercial nuclear power plants. An important attribute of the model is that it is sufficiently generic to permit its adaptation to application to the analysis of the impact of plant process performance on risk in other process industries. Model dynamics were verified to provide qualitative agreement, i.e. direction and relative magnitude, with the impact of process performance on risk that has been observed within the commercial nuclear industry and is judged to provide useful risk insights that can be used to obtain practical process improvements. Therefore, the model intentionally does not provide a quantitative link between the impact on plant risk due to plant process performance and the risk estimated in a PRA.

Further analysis using both analytical and numerical techniques has been performed to obtain additional verification of the validity of the model and to obtain additional insights. These include detailed analysis of the impact of the specific risk mitigating functions (equipment reliability and loss prevention) on plant risk, the potential for system bifurcations and entrance into unstable operational regimes to occur, addition and analysis of the impact of plant risk culture, and the impact of additive noise. Results obtained from the conduct of these studies will be provided in a subsequent paper.

Acknowledgements

The authors wish to recognize the Electric Power Research Institute for providing the funding for this research.

References

[1] Fleming KN. Issues and recommendations for advancement of PRA technology in risk-informed decision making. NUREG/CR-6813. Washington, DC: United States Nuclear Regulatory Commission; 2003.

[2] May RM. Simple mathematical models with very complicated dynamics. Nature 1976;261.

[3] Saperstein A. Chaos and the making of international security policy. In: Krasner S, editor. The ubiquity of chaos. Washington, DC: American Association for the Advancement of Science; 1990.

[4] Grossman S, Mayer-Kress G. Chaos in the international arms race. Nature 1989;337:701.

[5] Saperstein A. Chaos: a model for the outbreak of war. Nature 1984; 309:303.

[6] Saperstein A. Dynamical modeling of the onset of war. Singapore: World Scientific; 1999.

[7] Mintzberg H. The structuring of organizations: a synthesis of the research. Englewood Cliffs, NJ: Prentice-Hall; 1979.

[8] Apostolakis G. Organizational factors and nuclear power plant safety. In: Misumi T, Wilpert B, Miller R, editors. Nuclear safety: a human factors perspective. London, UK: Taylor and Francis, Ltd; 1999.

[9] Gaertner J, Hess S. Achieving an effective living maintenance process: a handbook to optimize the process and keep it that way. EPRI TR-108774. Palo Alto, CA: Electric Power Research Institute; 1997.

[10] The standard nuclear performance model—a process management approach (Revision 3); 2002; Nuclear Energy Institute; Washington, DC

[11] Edelstein-Keshet L. Mathematical models in biology. New York, NY: Random House; 1988.

[12] Murray J. Mathematical biology. New York, NY: Springer; 1989.

[13] Brewer H, Gaertner J, O'Regan P. Nuclear plant safety risk management: a case study. In: Proceedings of PSA 2002 American nuclear society international topical meeting on probabilistic risk assessment. New York, NY: American Nuclear Society; 2002.

[14] CFR 50.65. Requirements for monitoring the effectiveness of maintenance at nuclear power plants. Title 10 Code of Federal Regulations Part 50 Section 65

[15] Alligood K, Sauer T, Yorke J. An introduction to dynamical systems. New York, NY: Springer; 1996.

[16] Gaertner J, Hess S. Assessing nuclear plant risk management effectiveness. In: Proceedings of the fourth American Nuclear Society international topical meeting on nuclear plant instrumentation, controls and human–machine interface technologies. La Grange Park, IL: American Nuclear Society; 2004.

[17] Hess S. Assessing nuclear power plant risk management effectiveness. EPRI Report 1008242. Palo Alto, CA: Electric Power Research Institute; 2004.

[18] Hess S, Gaertner J. Investigation of nuclear plant safety utilizing an analytical risk management model. In: Spitzer C, Schmocker U, Dang V, editors. Proceedings of probabilistic safety assessment and management (PSAM7). London, UK: Springer; 2004.

[19] Bley D, Kaplan S, Johnson D. The strengths and limitations of PRA: where we stand. Reliability engineering and system safety. 38.: Elsevier Science Limited; 1992.

[20] Davoudian K, Wu J, Apostolakis G. Incorporating organizational factors into risk assessment through the analysis of work processes. Reliability engineering and system safety. 45.: Elsevier Science Limited; 1994.