NBS Enterprises
IT Services & Predictive Analytics

WOMAN-OWNED SMALL BUSINESS (WOSB) … VIRGINIA CERTIFIED SWAM

Information Technology and Network Dynamics

NBS Enterprises, LLC Proprietary

Natasha J. Schebella
CEO, President & Owner
703-851-0233
nschebella@nbsenterprise.com

Gary S. Schebella
Chief Scientist
703-999-1849
garyschebella@nbsenterprise.com

12 ½ S. King Street, Leesburg, VA 20175
Phone: 571-258-1616 … Fax: 571-258-1617
Website: www.nbs-advantage.com

Table of Contents

INFORMATION TECHNOLOGY AND NETWORK DYNAMICS 1
Introduction *1*
ITIL Best Practices *2*
Data-to-Models Paradigm *3*
Network Dynamics *4*
Data Management *5*
Cyber Security *6*
Transition Strategy and Business Process Reengineering *7*
Physical Security *8*
APPENDIX A: TOOL SUITE THEORY 1
Analytical Tool Suite *1*
APPENDIX B STUDIES AND ANALYSIS 1
Decision Support *1*
Domain Optimization *1*
Requirements Analysis *1*
Transitions between Models *2*
Optimization and Performance Assessment *2*
Technology Assessments *2*
APPENDIX C: TRANSITION STRATEGY AND BUSINESS PROCESS REENGINEERING 1
Using the "As-is" System as a Basis for the "To-be" Design *4*
Applications and Benefits *6*
APPENDIX D: CYBER SECURITY 1
Benefits *1*
Process Model and Superior Performance *1*
Mapping of Measurements and Risk Assessment Results *2*
Concept of Operations *2*
Metrics *3*
Data Recordings *3*
Analytical Forecasting and Enhancements of Operational Procedures *3*
Prioritization of Measurements *3*
Graceful Degradation *4*
Modeling Results and Prioritization *4*
APPENDIX E: THE DATA-TO-MODELS PARADIGM 1
Model Transition *2*
APPENDIX F: PHYSICAL SECURITY 1
Testing and Review *1*
Black Box Testing *1*
Review Execution and Planning *1*
Surge Methodology *1*
Routine Vulnerability Scanning *1*
Enhanced Assessment Capabilities *2*
Password Cracking *2*
Vulnerability Tracking *2*
Vulnerability Notifications *2*
Vulnerability Remediation *2*

NBS Enterprises
IT Services & Predictive Analytics

INFORMATION TECHNOLOGY AND NETWORK DYNAMICS

Introduction

Software and systems development is as much of an art as it is a science. Unfortunately, many aspects of a true development science have been ignored in favor of intuition. The results, as exemplified in the evolving government health insurance applications system, are costly and fraught with errors. In response to the many large-scale projects, which are terminated for lack of progress, NBS Enterprises (NBS) has developed a process that is based upon rigorous mathematical paradigms. It goes beyond AGILE and other representation and testing schemes by transitioning qualitative associations to quantitative models. The models when exercised produce performance, traceability and system/ software optimization. Given that development follows the modeling guidance, a final product performs as desired.

The process model implements a spectrum of interactive techniques described in the remainder of this paper

- General software development
- System/ software representation and modeling
- Dynamic network analysis
- Business process reengineering
- Data management
- Cyber security
- Physical security

Exhibit 1 depicts the integration of the NBS system/ software development tool suite. Management of projects is conducted with the use of ITIL. The AGILE methodology is employed for reviews and testing. UML represents all aspects of a project and is mapped to quantitative models. Cloud environments assist with the management of data.

The models are exercised to provide performance analysis, traceability, and optimization. A business process reengineering paradigm serves to convert as-is systems to to-be systems. As opposed to repairs during testing and operations, applications of the NBS methodology and tool suite assist with the discovery and rectification of errors during the development cycle. As a result, costs are reduced, functional requirements are existent in a design, and desired performance is ensured.

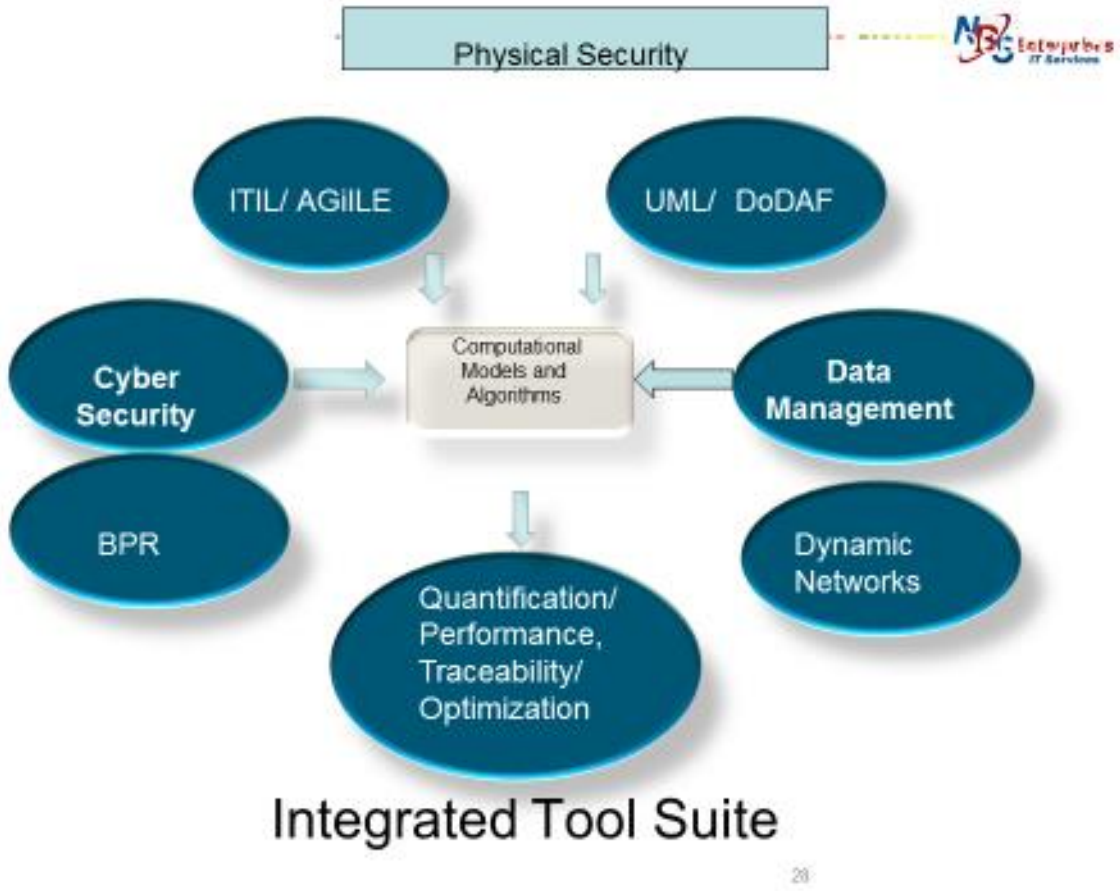


Exhibit 1

ITIL Best Practices

The NBS technical approach to development is built on the foundation of Information Technology Infrastructure Library (ITIL) best practices. NBS has a long history of supporting these procedures. NBS does not bring cookie-cutter performance or management tools with us and try to push a customer into a one-size-fits-all solution. We bring a methodology of examining and supporting all facets of an IT project, including development, management, operations and reporting. This global view of the ITIL model and the NBS technical philosophy is presented in Exhibit 2.

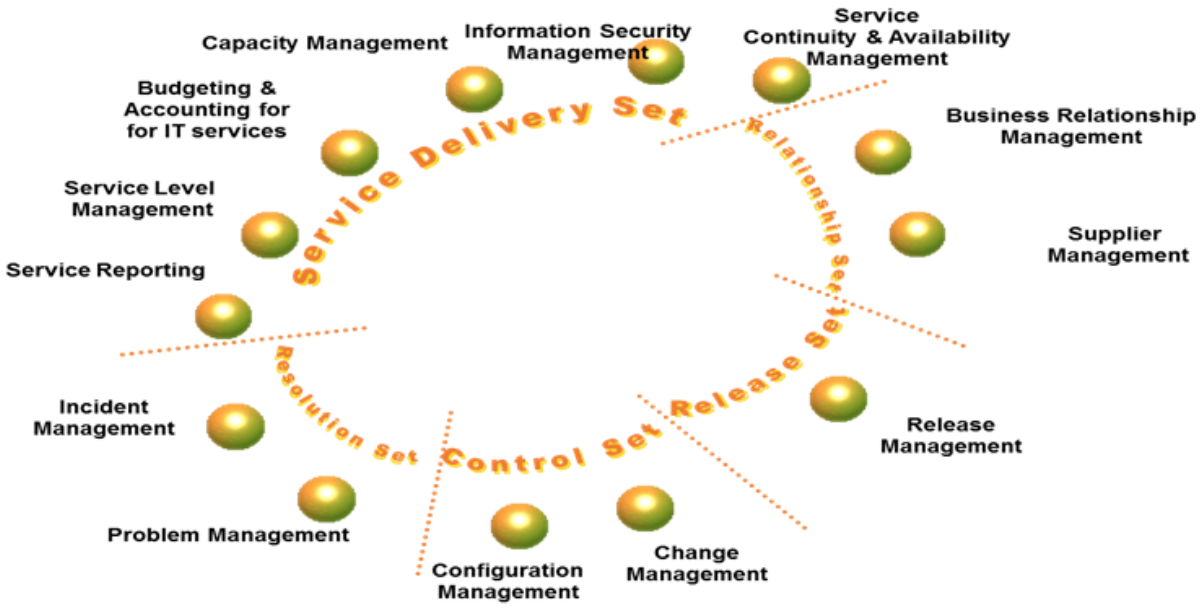


Exhibit 2

The ITIL elements encapsulate an overarching concept to manage all sub-tasks to support a project. While each of the sub-tasks involves change, a single change management process is used to review, approve and monitor releases. A single incident management process, taught to all staff members in a consistent manner, ensures that any problem in any sub-task is discovered, escalated, resolved and reported in a standard format. Wherever possible, service level measures are initiated to provide objective feedback on performance for all activities, including planning, financial management, application development and user support. This built-in feedback loop provides objective evidence of performance and gives NBS the opportunity to not only provide superior service but to improve service over time by fine-tuning performance of a project.

Data-to-Models Paradigm

The NBS approach to software development encapsulates ITIL for management, the AGILE methodology as a process model, Department of Defense Architectural Framework (DoDAF) and Unified Modeling Language (UML) for representation, and quantitative analysis with performance computations. All of the methods and tools are integrated into flow of information and decision support.

The Department of Defense (DoD) has promulgated a detailed process to develop architecture frameworks for system representations: DoD Architecture Framework (DoDAF). Once reaching an appropriate stage of definition, selected outputs from these frameworks serve as cornerstones for system design and development of complex systems. Architecture is defined as: “The structure of components, their relationships, and the principles and guidelines governing their design and evolution over time.” Further, “The DoDAF provides the guidelines

and rules for developing, representing and understanding architectures based on a common denominator across DoD, and Joint and multinational boundaries. The DoDAF ensures that architectural descriptions are compared and related across programs , mission areas, and ultimately the enterprise, thus, establishing the foundation for analysis that supports decision-making processes throughout DoD." The DoDAF encapsulates several architectural views. These comprise an All View, an Operational View, a Systems View and a Technical Standards View. A reflection of each view is described in the dynamic properties of an evolving system. In many cases, other modeling languages are employed to amplify decision points and system dynamics. Two of the most popular languages are Unified Modeling Language (UML) and Information Definition (IDEF). UML is an object oriented language best suited for software projects. IDEF implements structured analysis normally applied to business processes. To fully understand the impact of operational and systems rules and the dynamics of an implemented system, modeling and simulation are necessary to compute performance statistics for all artifacts of a proposed system. Further, the impacts of current and forecasted technologies need to be assessed. Numerous tools and simulation languages are available for applications. However, a commercial-off-the-shelf (COTS) tool which encapsulates the capabilities to generate both performance calculations and the optimal disposition of system components is not available on the open market. The NBS tool suite, when applied, saves think times, operational costs, and enhances robustness and performance. It has the potential to map directly from UML and IDEF models. A transition is made from qualitative descriptors to a representation suitable for performance and optimization calculations. The tool suite was conceived, developed and tested to provide a quantitative design process for complex, distributed systems. Granular levels of representation are obtained which contribute to the understanding, robustness, and security of an information technology system.

Network Dynamics

Distributed, large-scale information technology (IT) networks are accessible in many forms across the internet. These networks are highly integrated so that failure at one location might impact the performance at one or more other locations. Given that a failure occurs, manual processes are initiated to isolate the cause and to schedule maintenance procedures. Some automated measurements are provided by the networks themselves while human investigations occur simultaneously. In some cases, machine measurements are ignored by managers and staff. Consequently, failure data are difficult to interpret, and manual assessments are time consuming and not always accurate. Because of these inefficiencies, networks experience extensive downtimes, maintenance tasking and scheduling might be faulty, and repair costs are excessive.

In addition to real-time failures, a network and its components in many cases do not function as desired nor are their deficiencies readily apparent. Rather than searching randomly for enhancements that will improve performance, accurate analytical models of a network are necessary to identify bottlenecks and to employ optimization techniques to recommend corrective courses of action automatically.

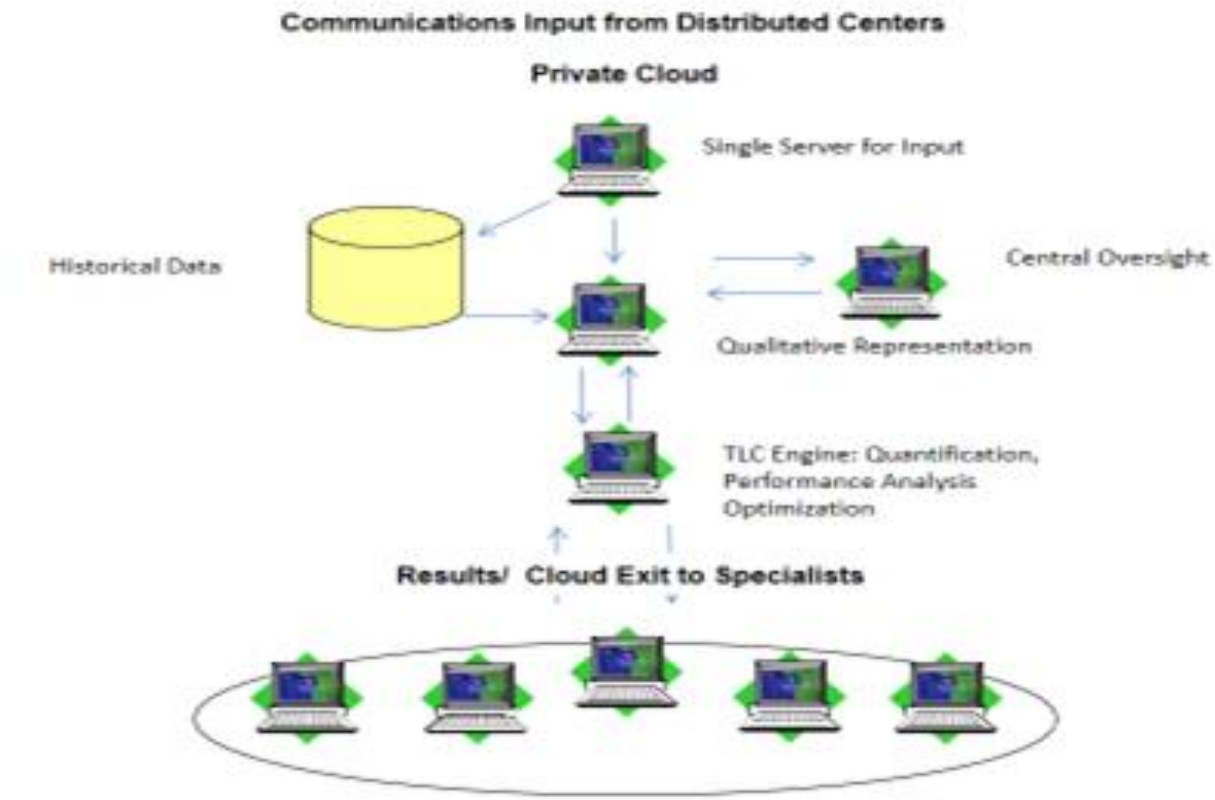
Automated decision support is required in order reduce assessment timelines. A means of associating machine measurements and human assessments contributes to evaluator think time reductions. In order to make intelligent decisions, analytical models are required to represent all components of the networks. By exercising the models, performance statistics are computed which address risk assessment, graceful degradation, and enhancement prioritizations. Courses of action (COA) for "fix-it" routines and scheduling are provided. Not only is think time reduced, but also the mean time to repair is minimized and incremental builds to gradually enhance performance are prioritized.

NBS has applied the network representations not only to real-time operations but also as a target for the DoDAF/ UML qualitative descriptors. Consequently, performance statistics are generated continually providing feedback to developers. The computational results produce performance statistics, traceability, areas of risks and guidelines for graceful degradation. Software engineers and programmers are able to insert effective changes as a system and software are in development, as opposed to later fixes during testing.

Data Management

Cloud architectures are now state-of-the-art. NBS has developed efficient systems in the commercial world. As an example, the Kohl's Department Stores employ the NBS solution to their data management. In the past, their online ordering system was overloaded during Christmas. It crashed producing a major loss in sales. The current cloud environment does not experience overload and is a resolution to holiday traffic.

Exhibit 3 shows a view of a typical cloud architecture.



Composite Architecture: Business Process Reengineering

Exhibit 3

Cyber Security

NBS cyber security tool suite does not employ measurement tools. Rather, it uses the results of measurements as input to a decision support system (DSS) that prioritizes detection types, reflects all aspects of operations, assists with graceful degradation and control, and provides a global view of threat impacts and information system performance in near real-time.

Current processes and technology hinder manager and staff abilities to manage large-scale information technology (IT) systems and to develop and execute courses of action in response to cyber security conditions. Extensive data and variables must be factored into a decision process. Time lines, mission characteristics and command, control, and communications (C3) performance might not be well defined. Labor intensive processes, in many cases, require several person hours to develop a course of action (COA). A nonlinear, asynchronous solution space, under current conditions, produces inaccurate stovepipe results. In addition, a response to ongoing events not only relies on organic detections within an IT system purview, but also actionable intelligence from external sources. However, a flood of

collected data has seriously degraded the timely assessments of cyber information and the identification of high-value quanta of information. An obvious, but difficult solution is to automate as much of an evaluation process as possible while still retaining the expertise of human judgment. Steady improvements in data access rates and formatting have been realized with data warehouse technology. Data mining has similarly enhanced decision support models. Still lacking is a comprehensive decision support system (DSS) that associates measurements of intrusions with operational data.

The primary challenges of developing computational models for a DSS are:

- Identification and prioritization of intrusion types.
- The structuring of detections for input to a system context model and an integration with other modeling variables
- The representation of context models that will accept all relevant data inputs and provide quantitative mission information.
- The NBS paradigm encapsulates all three challenges into a real-time DSS available to assist with management decisions and to provide near real-time courses of action. Measurements are processed continually as they are recorded minimizing responses to harmful intrusions.

Transition Strategy and Business Process Reengineering

Numerous large-scale, complex systems are noted to fail in their infant state. The number of errors within an inefficient design require changes that drive the cost of implementation well beyond an initial price tag. Errors and false starts are not only common to information systems, but also mature enterprises that are attempting to cope with change. A few companies, such as Google, address the dynamics of consumer choices in a well regulated manner resulting in the growth of profits and customer satisfaction. However, others experience a surge in stock prices only when a chief executive decides to retire.

To revamp a business process in response to change requires extensive planning. How to plan is entirely optional, but the possibilities are noted by a famed economist:

> "It is a dispute about whether planning is to be done centrally, by an authority for an entire enterprise, or to be divided among many individuals."
> Fred Hayek

The NBS business process reengineering paradigm comprises a set of software tools that encapsulate both centralized and distributed planning. Further the tool suite transitions qualitative design representations to quantitative models, assists with the transition of as-is to to-be systems, and provides recommended courses of action for changes of a business process.

Physical Security

In addition to cyber security, the physical confines of an information technology system must be protected with many aspects of physical security.

NBS conducts technical application, infrastructure, and component level security testing, network based penetration testing and specialized security and privacy reviews of software and hardware. A thorough methodology using a combination of manual techniques as well as commercial tools, pinpoint specific vulnerabilities and underlying problems in the applications.

Application security assessments are applied to websites, web applications, client applications, mobile applications and software appliances. Unlike standard security assessments, the application assessment requires significantly greater human expertise to create application threat profiles and custom test cases. The application layer vulnerabilities fall into two broad categories, the technical vulnerabilities like SQL injections and Cross Site Scripting and logical vulnerabilities that lead to illegal transactions and privilege escalation. A security assessment plan specific to a customer addresses the vulnerabilities.

APPENDIX A: TOOL SUITE THEORY

Analytical Tool Suite

The NBS software tool suite that provides a representation scheme and a means to quantify computational models. The backbone of system representation is a general purpose problem solver (GPPS) that employs one network representation to permit the representation of semantic nets, performance computations, learning and value analysis (Exhibit A.1) A Petri net, which is the primary representation of the existing tool suite, is a rule-based encapsulation of a network or any complex system. Optimization is always accomplished in the context of a systems model. Only one measure of effectiveness is optimized while all system variables are balanced to best achieve an objective. The variables represent competing measures of performance such as maximum impact of an event versus time of event execution. Either maximum impact or timing can be emphasized, or combinations of the two can be obtained.

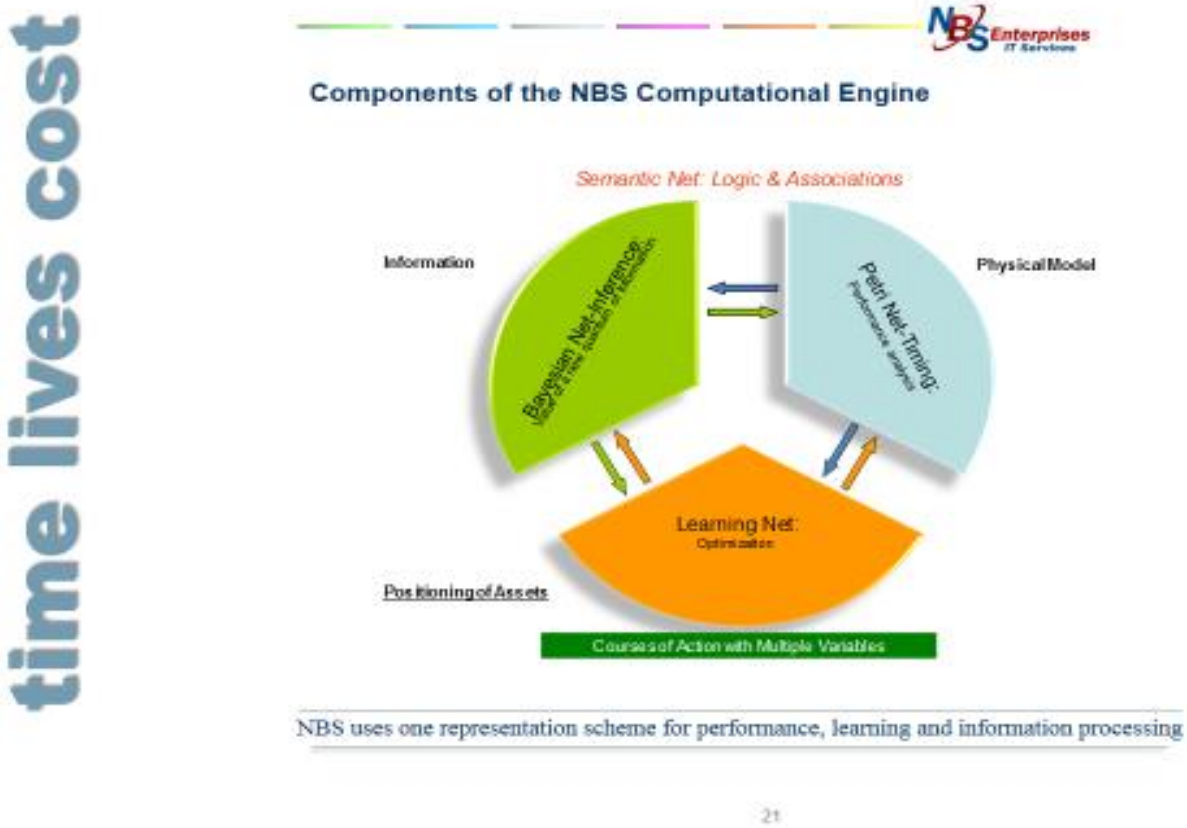


Exhibit A.1: Analytical Components of the Tool Suite

Performance Modeling

The motivation to use Petri nets as a prime representation scheme results from their power to act as a rule-based system and to be transferred easily into an analytical model or a simulation language.

Exhibit A.2 depicts the evolution from a system architecture to a Petri net and finally to a model that computes performance statistics. Initially, models are tested by developing challenge cases and comparing automated solutions to those generated manually. After thorough testing, the models are used for real-time computations in dynamic environments. The Petri net backbone is then expanded by the super positioning of neural nets and Bayesian nets. One representation network has the potential to step through the triad of Figure A.1, producing performance statistics, optimization and value analysis, as well as an association of events with the use of semantic nets. By correlating execution time and variance with each event in a network, a Petri net is translated to an analytical model or a simulation language. The models are run to compute typical statistics such as response times, queue lengths, utilizations and throughputs.

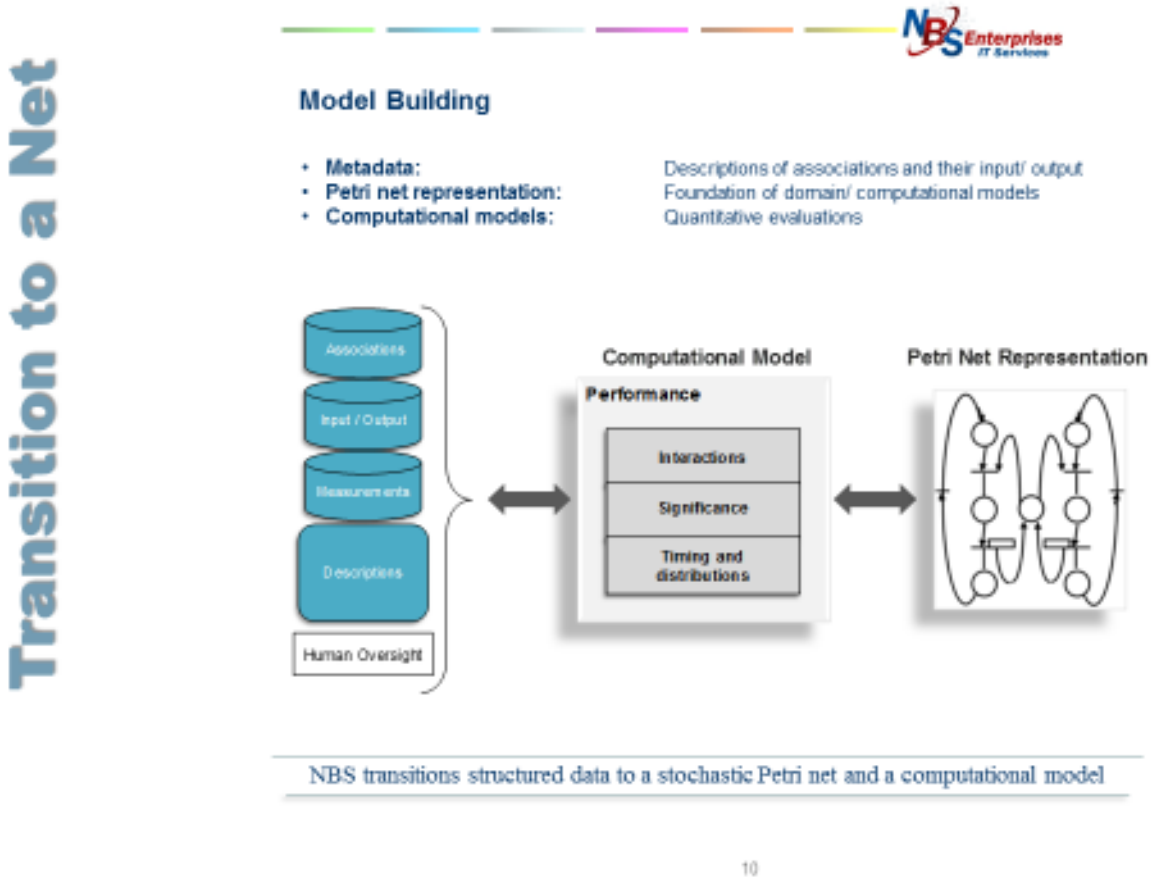


Exhibit A.2

Neural Nets and Optimization

The back propagation technique for neural nets is used for pattern recognition and other learning schemes. The incrementally changed weights associated with network links typically represent correlation statistics. For the composite nets, the weights in addition, signify performance statistics generated by a Petri net computation. For example, if an analyst is optimizing a communications flow, the weights indicate the quantities or latency by message type that are transmitted through each link and node. Back propagation is conducted in response to performance calculations until a "best" solution for message routing is achieved. An objective function might be the total latency of all messages in a network.

Information Increment and Value Analysis

The utility of Bayesian nets and statistical inference have been described by Judea Pearl: Probabilistic Reasoning in Intelligent Systems, Morgan Kaufman. The Pearl text is considered as a seminal description of statistical fusion and the representation scheme for networks of inference.

The approach is to transition Bayesian nets to Petri nets, which are a directed graph comprising conditions, transitions/ events and connecting links. By superimposing Bayesian nets onto Petri nets, the representation becomes time related and the assumption of event independence is minimized. The computational results provide a time-related, worth computation of an increment of knowledge.

NBS Enterprises
IT Services & Predictive Analytics

APPENDIX B STUDIES AND ANALYSIS

Decision Support

The NBS tool suite, in some instances, is applied during the planning stage of systems development and also for technology and concept evaluations. While system designers examine alternative architectures, processes and throughput solutions, estimates derived from data sources and physical components are used as inputs to the optimization and performance models. The assessment results are compared with mission requirements and if problems exist in a current concept or a new technology insertion, feedback of anomalies provides quantitative guidance relative to how a design might be improved. With this information, additional resources are applied precisely where they are needed most.

Domain Optimization

The optimization component of the hybrid semantic net comprises many techniques suited to a spectrum of problems. For distributed systems, resources are located optimally and sized for maximum effectiveness. Examples are as follows:

- Allocation of software to hardware.
- Allocation of personnel to tasks.
- Location of sensors and communication devices in a battlefield.
- Routes for vulnerability or time minimization of logistics and combat assets
- Distribution of messages in a communications network
- Replenishment and control of autonomous vehicles.
- Loading of transport vehicles.

In every case, an optimal configuration of resources is computed and related to a measure of system performance.

Requirements Analysis

Requirements analysis is a process of converting from an initial "as-is" architecture to a "to-be" architecture, or in other words, from what you have to what you need.

A hierarchy of qualitative models is provided that are transformed to quantitative models necessary for systems analysis. The models are structured as follows:

- a) Functional model: what a system is to accomplish
- Operational model: the tasks that instantiate functions
- Data and information models: distribution of data and decisions within a systems network
- Systems model: personnel, software and hardware contained in a system.
- Segment model: specifics of components such as a communications protocol

Transitions between Models

Each model is appended and enhanced to provide a subsequent model. For instance, a functional model is modified to show the specifics of tasking to generate an operational model. Operational models are embellished with the attributes of data and the location of decisions to provide data and information models. Quantitative analysis begins at any level of detail so that mathematics always supplements the architectural process. Operational analysis and systems analysis are combined to define the requirements of a suitable architecture.

An overview of requirements analysis, represented with the models discussed above follows:

- Obtain descriptions for a new or " as- is" architecture
- Identify functional requirements and workflow
- Identify the qualitative models noted previously beginning with a functional model and progress to other models as data become available
- Map all qualitative models to quantitative models
- Perform trade-offs, sensitivity analysis and comparative analysis with quantitative models to define a " to-be" system representation

Optimization and Performance Assessment

- Run the models and assess mission outcomes: as architecture models are defined and enhanced with attributes and greater levels of detail, computations are made to assist with the understanding of incremental architectural changes.
- Optimize by allocating the resources in a node (decisions, people, data, and processing): similar to assessment, optimization is accomplished as an architecture matures and not just for its final configuration.
- Carry out sensitivity analysis: during assessment and optimization, numerous examples are computed so that the sensitivities of parameters and variables are understood.

Technology Assessments

- Evaluate technologies (impact of physical systems): As the architectural models are populated, the attributes of competitive technological options are inserted into their proper nodes permitting a comparative assessment of their impact upon system performance.
- Look at tactics and management (blue timelines and tasks): the alternative means of conducting business within the system enterprise are assessed in the same manner as technologies. Assess system performance in terms of timing and requirements: assessments are made with respect to any interesting measure of performance such as cost or response time.

- Experiment with the catastrophic removal of nodes within a network and assist with the planning of operations: Nodes are removed and performance is computed in their absence. The results exemplify the capability of a crippled system. Further, the optimizer reconfigures a network by moving functionality and resources so that the best outcome is possible relative to catastrophic failures.

APPENDIX C: TRANSITION STRATEGY AND BUSINESS PROCESS REENGINEERING

The framework model, shown is Exhibit C.1, identifies a set of processes to define and integrate a system(s) within the context of an enterprise business process. The processes are shown as bounded and interrelated to the enterprise elements. The enterprise planning and management processes define the enterprise macro processes, identify the need for system components, and plan for the introduction into the enterprise environment. The enterprise data architecture and administration processes impose the data requirements and structures on the information architecture design. The enterprise business processes are supported by the information systems once they have been implemented into an operational environment. The effectiveness of the business processes is measured by selected metrics. Improvements are fed back into the system design through the enterprise management and planning process. This provides a closed loop set of processes between a business system and an enterprise process.

The framework model includes processes to define system architecture designs, develop the architecture segments, integrate the segments into a system, and operate and maintain the system and program management. This process framework model has been used to define, at lower levels, the set of interrelated processes identified. The processes are not limited to a single organization, but are true cross-functional processes. This framework is meant as a guide to move a company or large organization into a process-managed environment and away from operating by functional organizational activities. The process framework model is a summary model that does not describe the detailed relationships between processes and does not identify the products of the processes. The cross-functional teams that define the processes define the relationships and products.

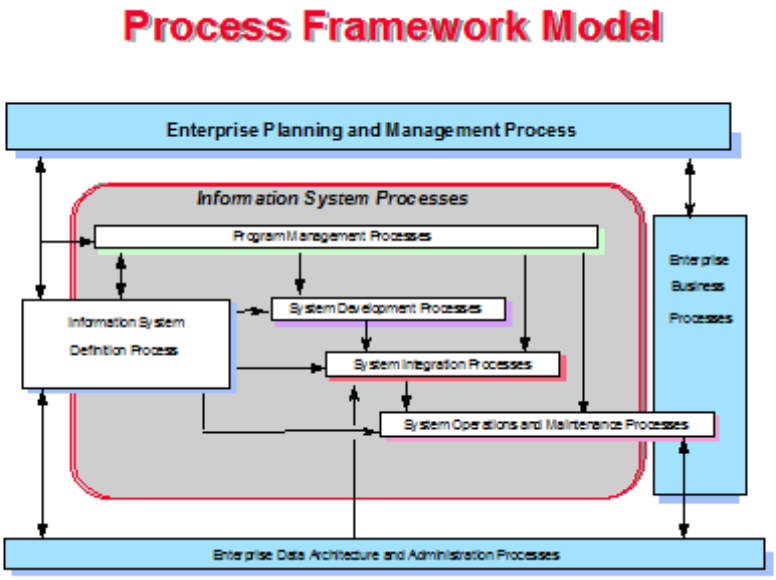
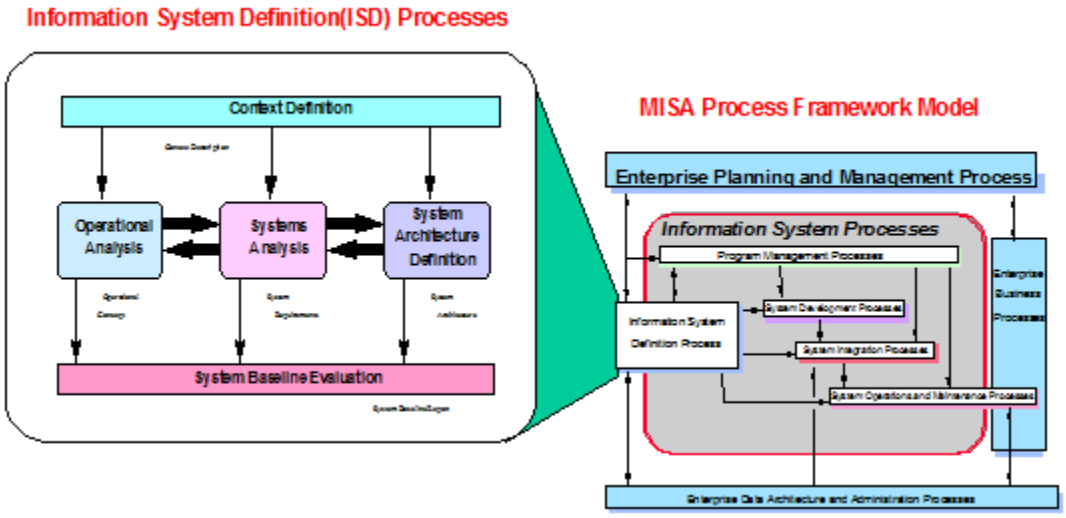


Exhibit C.1 - The process framework model identifies the processes and their relationship for managing business systems.

Within the process framework model, the linkage to the business process and the definition of the architecture is accomplished through the Innovative System Definition (ISD)

process. Exhibit C.2 shows the ISD process within a management information system architecture (MISA) Process Framework Model. The ISD process includes sub processes for establishing the system context, performing an operational analysis, performing system analysis, defining the system architecture, and establishing a system baseline. The linkage with the business process is accomplished by identifying the system context within the enterprise business processes. The Operational Analysis process also performs linkage. The Operational Analysis process is used to reengineer, or define, the business process. However, it does much more than just create a business process model. It creates a process model, data models, location models, operational sequence diagrams, operational scenarios, user profiles, operational timelines, and an operational cost analysis. The Systems Analysis process is used to analyze the operational concept and define the requirements that must be satisfied by the system architecture. The system analysis process is also used to create several analytical models. These models include functional, architecture and performance models. The System Architecture Definition process is used to define an architecture that satisfies the operational concept and its requirements. The System Baseline Evaluation process is used to ensure that all required documentation is completed, that all requirements are satisfied, that a technical management plan is developed, and that areas of risk are identified and a risk management plan is developed. The principal product from the ISD process is a system architecture definition.



The Information System Development Process links the Entire Enterprise processes to the information systems.

Exhibit C.2 - Baseline Definitions

The development of a system architecture is a very complex process requiring many skills. Because of the many skills required, a process is essential to addressing all of the areas and issues. The resulting architecture is the deciding factor for system performance, the operational and maintenance cost for the system life cycle, and the enabling or preventing mechanism for making system and process changes. Therefore, the process for defining the

system should have key principles that make the process work for the people with different skill areas that must use it, and also result in an architecture that meets the objectives desired. The ISD process has the following principles:

- **Architecture Hierarchy Decomposition** - The ISD process uses the hierarchical decomposition of the architecture from an enterprise level down to an information system level, then to subsystem levels and finally to a component level. Each level of decomposition increases in detail. The output product from each level of the ISD process becomes the input to the next level of decomposition. Each level of decomposition produces a more detailed set of output products. By having the architecture description structured in layers, when changes to the system are required, the process can be entered at any level. This allows the architects, or designers, to make changes at a component or subsystem level without a complete system redesign, because the architecture is structured and documented within the context of the other elements within the layer and with the decomposition from the layer above and to the layer below. This also allows system models to be built at an upper level and decomposed to lower level models. By having the models at the various levels gives the flexibility to easily change portions of the business process. This flexibility is necessary since the infrastructure will typically change more frequently than the business processes.
- **Transformation from process to architecture** - Business process definition, or re-engineering can, and often does occur separately from the system architecture definition. However, the best systems are built when personnel with all the various required skills are formed into an integrated team. The ISD process has been developed with the concept of using integrated teams. Therefore, the ISD process includes a sub-process to perform the operational analysis and define the business processes at lower levels that correspond to levels of architecture design. The business processes then drive the architecture design.

This transformation from a business process to an architecture design is where the business process engineering tools and methodologies generally fail. Many authors and processes recognize business process reengineering and system decomposition, but a method of transformation from business processes to architecture is not addressed. The ISD process includes all three elements as sub processes: (1) business process design, or reengineering, (2) architecture hierarchical decomposition, and (3) transformation. Exhibit C.3 shows these three elements in graphical form. The left parts of the triangle shows the business process definition (operational analysis process), the center shows the transformation (systems analysis process), and the right side shows the architecture (system architecture definition). The system analysis process is the process of defining the requirements for a system architecture that ensures the operational process/requirements are satisfied. The systems analysis process also develops analysis and models to ensure that the system architecture will indeed satisfy those requirements.

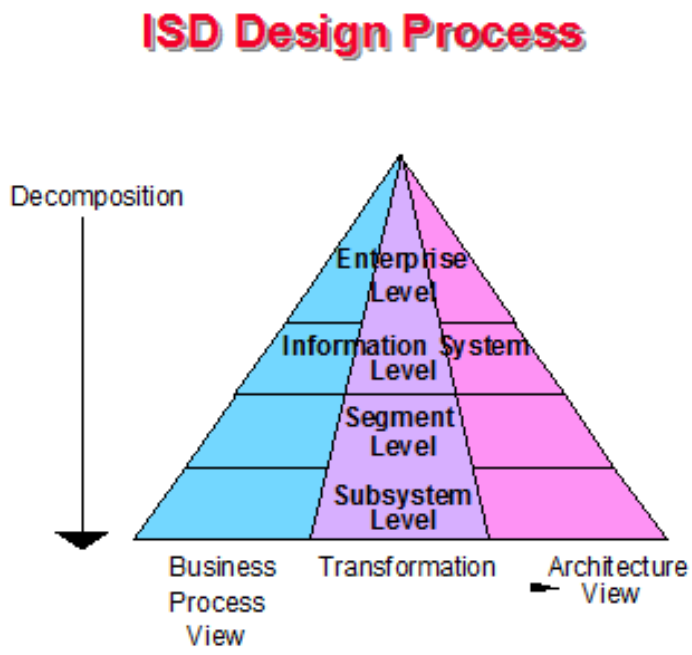


Exhibit C.3 -- The ISD System Design Process includes Business Process Reengineering, Architecture Hierarchical Decomposition, and Transformation.

Using the "As-is" System as a Basis for the "To-be" Design

The capturing of the "As-is" is part of the business process reengineering, normally referred to as reverse engineering. The "As-is" includes the business process, the operational processes, and the system architecture design. This activity helps identify the operational requirements. It also serves as a basis for developing migration and transition planning. The ISD process recognizes and includes this capability. In the decomposition of the operational analysis, system analysis, and system architecture definition processes, there are tasks for defining the "as-is" and "to-be" environments. The "as-is" business process is actually developed by reverse engineering of the "as-is" system architecture. This is because many of the old legacy systems simply automated manual processes. This is shown graphically in Exhibit C.4. As the islands of automation grows and is interfaced with the business process, it became "hard coded," nearly unchangeable, and undocumented except through the legacy information systems. The process of re-engineering business processes therefore often requires reverse engineering of legacy information systems; a hard and tedious task even with good documentation. Without documentation, this task can become nearly impossible if the systems are too large and/or complex.

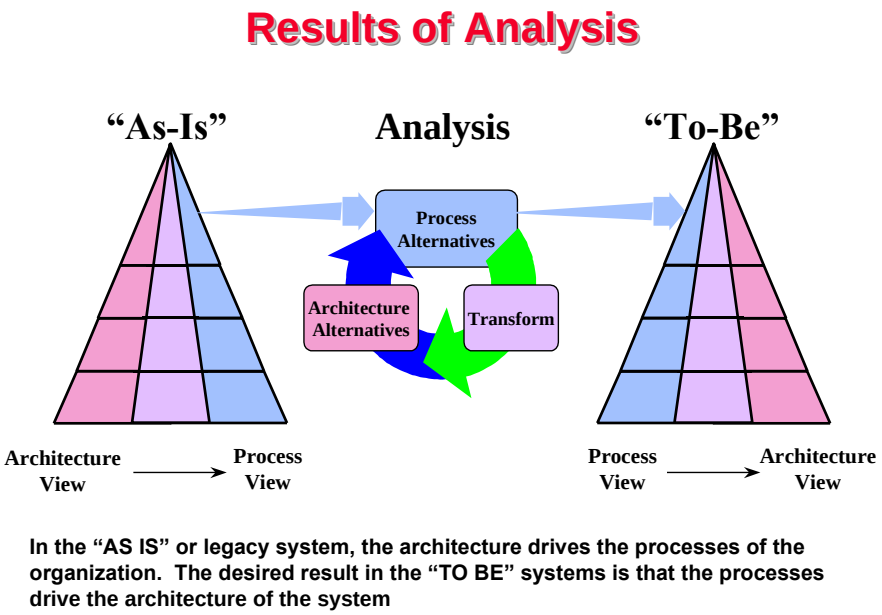


Exhibit C.4 -- The Analysis activity within each sub process transforms the "As-is" system to a "To-be" system.

Fortunately, in recent years, there has been substantial progress in the development of reengineering tools that can capture much of the "As-is" system. The tools analyze all objects, and in the process, capture the "As-is" architecture and produce quality documentation such as the data flow diagrams, structure charts, and the business rules. Extraction of this information is crucial to be able to make design changes.

- **System Analysis** - Within each of the ISD sub processes is a set of system analysis activities. One of the analysis activities is the performance of trade studies, or alternative analyses. These trade studies are used to identify and evaluate various alternatives. The sub processes are performed in conjunction, rather than the traditional sequential manner of most processes. Also the trade studies are not limited to elements of the architecture. Alternatives are first identified for the business, or operational processes, and evaluated in the Operational Analysis sub process to determine the preferred operational concept. The operational concept includes a system operational model that encapsulates activities and objects. The operational concept is then evaluated in the System Analysis sub process to determine technical feasibility and derived requirements. From the operational concept a requirement may be derived. The System Analysis sub process also develops functional models, data models, architecture models and performance models. The personnel performing the System Architecture Design sub process also participate in the development of the architecture and performance models. They

identify the specific elements of the architecture and the characteristics, or attributes, of the elements.

- **System Modeling** - The ISD process includes defining a set of system models. The models include the business process, the operational processes, the functional models, the system architecture models, and the performance models. The number and type of models vary dependent on the size and complexity of a system. Although many tools can be used, the preferred tool is the NBS Time, Lives, Cost (TLC) tool suite that has been used on several large, complex systems. It is described in Section 3. It has been used primarily to develop system architecture models for the purposes of performance evaluation and alternative analysis of architecture structures. It has been very effective in matching existing system performance, identifying the cause of poor performance, and analyzing and predicting performance of alternative architecture changes. It constructs models using classical object oriented notation and representation.

Applications and Benefits

The ISD process can be used to design an individual business process, a set of processes, or a segment of a system. For any case, a transformation is made from an existing paradigm to a more efficient business model that reduces costs and enhances performance. The fundamental goal is the maximization of profits.

The process of forward engineering a system to produce a "To-be" system captures all of the models that describe business processes, information models, information system architecture, and the delivery systems. Hence, if a change of a system is contemplated, a "what if" analysis is performed to determine the impact of the change on the system. The "what if" analysis can be performed by the NBS reengineering tools and the system modeling tools. It results in a substantial increase in the stability of a system and, hence, increased user satisfaction and reduced costs.

The principal benefit is that the ISD process enables a company to undertake the challenge of making major changes to their enterprise and supporting those changes with a disciplined, proven set of processes and tools. It provides the visibility of the planned changes and new systems before actually beginning the effort or expending large amounts of resources and then discovering that the approach does not work. It supports the disciplined management of system architecture design and implementation.

APPENDIX D: CYBER SECURITY

The NBS decision support system (DSS) prioritizes detection types, reflects all aspects of operations, assists with graceful degradation and control, and provides a global view of threat impacts and information system performance in near real-time.

Current processes and technology hinder manager and staff ability to manage large-scale information technology (IT) systems and to develop and execute courses of action in response to cyber security conditions. Extensive data and variables must be factored into a decision process. Time lines, mission characteristics and command, control, and communications (C3) performance might not be well defined. Labor intensive processes, in many cases, require several person hours to develop a course of action (COA). A nonlinear, asynchronous solution space, under current conditions, produces inaccurate stovepipe results. In addition, a response to ongoing events not only relies on organic detections within an IT system purview, but also actionable intelligence from external sources. However, a flood of collected data has seriously degraded the timely assessments of cyber information and the identification of high-value quanta of information. An obvious, but difficult solution is to automate as much of an evaluation process as possible while still retaining the expertise of human judgment. Steady improvements in data access rates and formatting have been realized with data warehouse technology. Data mining has similarly enhanced decision support systems. Still lacking is the capability to effectively fuse diverse sources of information, to incorporate the essence of asynchronous events, and to propagate the belief of evidence in the context of time-dependent scenarios. The primary challenges of developing computational models for DSS are 1) identification and prioritization of intrusion types, 2) the structuring of detections for input to a system context model and an integration with other modeling variables, and 3) the representation of context models that will accept all relevant data inputs and provide quantitative mission information.

Benefits

Measurement tools for cyber security are readily available for the continual monitoring of system performance. But in addition, decision makers and their staff require an encompassing decision support environment to effectively manage large-scale information systems and to develop and execute courses of action in response to deleterious events.

The NBS paradigm produces a response to the results of measurements and the prioritization of those measurements. Measures of intruder performance (MOP) are defined and if they portray danger to systems operations, countermeasures are instigated immediately. Thus, a means is available to compute MOP and to prioritize detections of system intrusion. The foundation of countermeasures implementation is a continual source of measurements and the processing of their importance within a systems context..

Process Model and Superior Performance

The overall thrust of a decision making tool, which assesses the combined effects of operational components and measurements, is to transition data to performance models. Thereafter, the models are exercised to produce an analysis and a quantification of probabilistic

outcomes. Fundamentally, descriptions of system components, risk assessment results and asynchronous measurements are emplaced in a structured database. The database objects are mapped to sets of metadata that produces associations of measured events, their inputs and outputs (I/O), and times to respond to the events. Associations are further mapped to a context model that is exercised to provide courses of action.

Mapping of Measurements and Risk Assessment Results

Metadata provides rules for the association of timed or probabilistic events and their I/O, an automated mapping is visualized where first unstructured data are directed to an extraction tool suite. The extractor produces structured databases, which are transitioned by metadata to a definition of associations. The associations are further transitioned and positioned within a system context model that feeds analytical equations or a simulation of an IT system domain. By exercising the model, performance statistics are derived that encapsulate actions initiated by an asynchronous situation, as well as the context model, which represents an entire system of interest.

Concept of Operations

A concept of operations for an automated decision support system is outlined in Table 1. A context model is prepared for a domain. Many facets might be included in the context model such as IT assets and data flow within a network. Given that a new set of measurements is obtained, which describe detections of possible network intrusions, the ontology assists with a mapping to the context model. The context model is expanded to include the additional information and is exercised to display the impact of the change.

Table 1: Concept of Operations

- A risk assessment is established for an IT enterprise.
- Descriptions of risk are prepared for system components (locations of vulnerability, priorities, down times given a successful penetration, countermeasures).
- Metrics are defined and measurements are applied to vulnerable areas.,
- An analytical context model is defined to represent all IT system components and risk assessment factors,
- Impact, sensitivity and what-if analysis are conducted with the context model to provide analytical forecasting,
- Measurements of non-catastrophic events, failures and penetrations are recorded,
- Relevant asynchronous data are transitioned to a structured database.
- Metadata assist with the derivation of new associations which are mapped to the context model,
- The expanded context model is exercised to provide performance statistics (response times, impediments, uncertainties),

- Based upon performance statistics, countermeasures are recommended/ course of action,
- Measurements are processed continually to derive new courses of action.

Operations for the above scenario are accomplished within minutes as opposed to several hours of think time. Optimization functions are available for all possible violation types: physical, personnel, software, hardware, network, and data. The products of the automated decision support system contribute to reporting, the definition of tests, revisions to risk assessment, and a view of total system operations. Vulnerabilities, in and by themselves, in many cases are misconstrued, whereas a global representation of vulnerability interactions clearly identifies the most critical regions of system compromises. Further, countermeasures to potential or actual threats are displayed automatically for view by IT managers.

Metrics

The selection of metrics for performance measures is an ongoing and volatile pursuit. First, metrics differ for various levels of personnel. Management might be interested in measures of costs and downtime, while technicians are more concerned with measures such as failures per unit time. Regardless, measurements and recordings of results are hierarchical. The metrics must correlate with the hierarchy. Initially, measurements are made for a high-level phenomenon such as mean number of penetrations per unit time. Thereafter, granularity ensues: penetrations of type A, penetrations of type B, etc. Special categories of a penetration type might also be necessary.

Data Recordings

Measurements are recorded electronically as they are obtained in the format specified by an enterprise. The time, place and type of measurement are stored in a relational database so that reports are generated on a periodic basis. Further, dashboard displays are available for personnel observations. SQL queries are made so that the nature of measurement results is readily available. Measurements of effectiveness are derived from measurements and metrics so that system and component performance is defined for any point in time.

Analytical Forecasting and Enhancements of Operational Procedures

A measures and metrics leader continually reviews all measurements, decision support results and feedback from system operators to provide analytical forecasting and recommendations for new measurement applications.

Prioritization of Measurements

From the aspect of intruder operations, the NBS algorithms are able to accept descriptions of viral behavior and the potential to cause damage to specific nodes within a network. Qualitative descriptions are transitioned to quantitative representations which are exercised by the algorithmic tool suite. The results probabilistically bound potential outcomes of intrusions. A contributor to countermeasures is the development of intruder measures of

performance so that a prioritization of detection types is possible. Time critical courses of action are formulated in response to serious cases, while less significant detections are addressed at a more leisurely pace.

Graceful Degradation

The quantification of network nodal interactions begins with the development of a model from descriptions of processing, connectivity of nodes and communications. Examples of selected parameters include definitions of all devices, locations of nodes, protocols, concepts of operation and physical phenomena of a threat. Dynamic changes are imposed in an asynchronous manner upon network components. Changes in a model follow directly from changes in an IT system. If a node is compromised, it is deleted from a network representation. A new performance is computed using the reduced model. Thus, a network's response to intrusions is quantified and optimization components of the tool suite provide revised operations.

Modeling Results and Prioritization

Once a model is represented, it is exercised to provide network performance results. Thereafter, an asynchronous event is injected into the model. Table 2 relates modeling results to the information required for detection prioritization.

Table 2

Modeling Statistic	Significance of the Statistic
Throughput at a node generated by an insert	Probability that the impact of an insert reaches a particular node
Timing	Time required for an insert to reach a node
Secondary throughput	compromised node and sent to other nodes
Mean time to repair	Time to repair a compromised node

The value of a function within a network is established in two ways: 1) value established by a heuristic judgment, and 2) by modeling results. Given functional failure, the reduced performance of a network is quantified. Nodal downtime for a function is indicated by the mean time to repair. To further instantiate the prioritization, information through risk analysis is made available. The information comprises estimates of which functions might be compromised given an intrusion of type X. A measure of performance (MOP) for prioritization can require combinations of more than one statistic. Interest might exist for multiple MOP such as mean time to repair, propagation time of a virus through a network or reduced system performance. An NBS paradigm exists which combines two or more MOP into a single measure of effectiveness (MOE).

APPENDIX E: THE DATA-TO-MODELS PARADIGM

The NBS approach to software development encapsulates ITIL for management, the AGILE methodology as a process model, Department of Defense Architectural Framework (DoDAF) and Unified Modeling Language (UML) for representation, and quantitative analysis for performance computations. All of the methods and tools are integrated into flow of information and decision support.

The Department of Defense (DoD) has promulgated a detailed process to develop architecture frameworks for system representations: DoD Architecture Framework (DoDAF). Once reaching an appropriate stage of definition, selected outputs from these frameworks serve as cornerstones for system design and development of complex systems. Architecture is defined as: "The structure of components, their relationships, and the principles and guidelines governing their design and evolution over time." Further, "The DoDAF provides the guidelines and rules for developing, representing and understanding architectures based on a common denominator across DoD, and Joint and multinational boundaries. The DoDAF ensures that architectural descriptions can be compared and related across programs , mission areas, and ultimately the enterprise, thus, establishing the foundation for analysis that supports decision-making processes throughout DoD." The DoDAF encapsulates several architectural views. These comprise an All View, an Operational View, a Systems View and a Technical Standards View. A reflection of each view is described in the dynamic properties of an evolving system. In many cases, other modeling languages are employed to amplify decision points and system dynamics. Two of the most popular languages are Unified Modeling Language (UML) and Information Definition (IDEF). UML is an object oriented language best suited for software projects. IDEF implements structured analysis normally applied to business processes. To fully understand the impact of operational and systems rules and the dynamics of an implemented system, modeling and simulation are necessary to compute performance statistics for all artifacts of a proposed system. Further, the impacts of current and forecasted technologies need to be assessed. Numerous tools and simulation languages are available for applications. However, a COTS tool which encapsulates the capabilities to generate both performance calculations and the optimal disposition of system components is not available on the open market. In response, NBS has developed an evolving tool suite which provides multiple capabilities. When applied, the tool suite saves think times, operational costs, and enhances robustness and performance. It has the potential to map directly from UML and IDEF models. A transition is made from qualitative descriptors to a representation suitable for performance and optimization calculations. The tool suite was conceived, developed and tested to provide a quantitative design process for complex, distributed systems. Granular levels of representation are obtained which contribute to the understanding, robustness, and security of an information technology system.

To supplement DoDAF, NBS has developed a comprehensive analytical tool suite and system/ software models that provides traceability, performance analysis, and optimization of an architecture during development. Granular levels of representation are obtained which contribute to the understanding, robustness, and security of an information technology system.

A representation and planning system is instrumental in the understanding of computer code and diverse technological components and their performance relative to functional requirements. Necessary capabilities are:

- reasoning with uncertain information
- representation of data at different levels of granularity
- performance analysis and optimization
- traceability
- rapid capture of change
- automated courses of action

Model Transition

Exhibit E.1 shows the flow and transition of data-to-models.

Data of various types in the form of video, text and numbers are collected and transformed to a format that the NBS tool suite is able to process.

The tool suite produces a model that replicates a physical system in mathematical terms. By exercising the model, performance statistics are generated (how well does a system work?). The model also optimizes a system (How things can be made better). As new data are generated, the system learns and continually provides answers to queries. The process differs in that it is able to not only measure performance and to optimize simultaneously, it also provides forecasting of what courses of action are required now and in the future. As long as data are input, processing never stops.

Each flow of unstructured data is transformed into a format that is compatible with a common representation scheme. A separate, structured database is composed for each data stream and is given the characteristics of metadata. A metadata element is operated on by a unique set of rules creating associations for any asynchronous event of significance. The associations are produced in a continuous mode. Once new associations become available, dependencies with other associations are identified, as well as timing statistics: means and variances for event completions. The associations are inserted into a context model which represents an entire scenario of interest: assets, timelines, and dependencies. The context model is exercised producing performance statistics and impact analysis. In addition to a general context, optimization algorithms are appended. The additions address specific issues such as where, when, and against whom to conduct a counter action. Based upon the results of analysis and optimization, a course of action, with a rationale for selection, is presented for consideration to a decision maker.

Data of various types in the form of video, text and numbers are collected and transformed to a format that the NBS tool suite is able to process.

The tool suite produces a model that replicates a physical system in mathematical terms. By exercising the model, performance statistics are generated (how well does a system work?).

The model also optimizes a system (How things can be made better). As new data are generated, the system learns and continually provides answers to queries. The process differs in that it is able to not only measure performance and to optimize simultaneously, it also provides forecasting of what courses of action are required now and in the future. As long as data are input, processing never stops.

Each flow of unstructured data is transformed into a format that is compatible with a common representation scheme. A separate, structured database is composed for each data stream and is given the characteristics of metadata. A metadata element is operated on by a unique set of rules creating associations for any asynchronous event of significance. The associations are produced in a continuous mode. Once new associations become available, dependencies with other associations are identified, as well as timing statistics: means and variances for event completions. The associations are inserted into a context model which represents an entire scenario of interest: assets, timelines, and dependencies. The context model is exercised producing performance statistics and impact analysis. In addition to a general context, optimization algorithms are appended. The additions address specific issues such as where, when, and against whom to conduct a counter action. Based upon the results of analysis and optimization, a course of action, with a rationale for selection, is presented for consideration to a decision maker.

Data Transformations

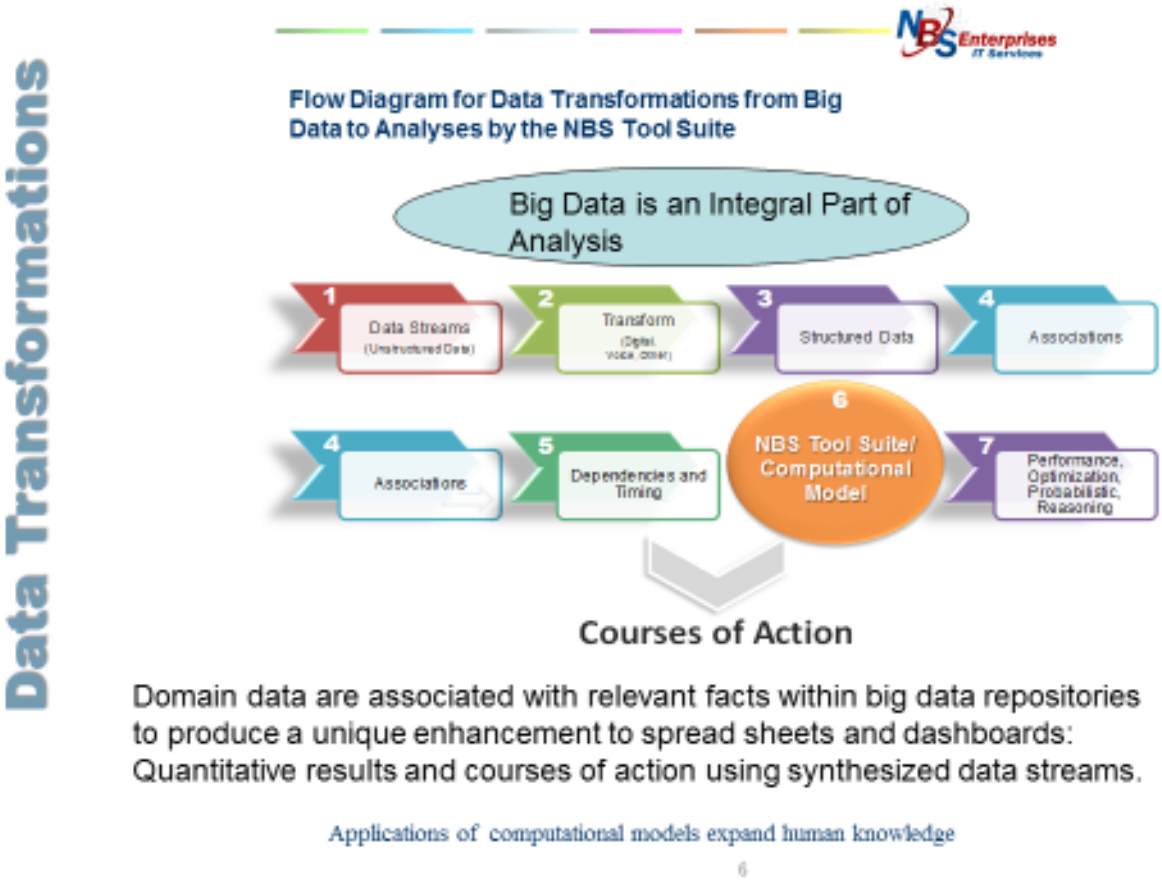


Exhibit E.1

NBS Enterprises
IT Services & Predictive Analytics

APPENDIX F: PHYSICAL SECURITY

Testing and Review

In addition to cyber security, the physical confines of an information technology system must be protected with many aspects of physical security.

NBS conducts technical application, infrastructure, and component level security testing, network based penetration testing and specialized security and privacy reviews of software and hardware. A thorough methodology using a combination of manual techniques as well as commercial tools, pinpoint specific vulnerabilities and underlying problems in the applications.

Application security assessments are applied to websites, web applications, client applications, mobile applications and software appliances. Unlike standard security assessments, the application assessment requires significantly greater human expertise to create application threat profiles and custom test cases. The application layer vulnerabilities fall into two broad categories, the technical vulnerabilities like SQL injections and Cross Site Scripting and logical vulnerabilities that lead to illegal transactions and privilege escalation. A security assessment plan specific to a customer addresses the vulnerabilities.

Black Box Testing

Black box testing and Security verification is performed by using methods, tools and styles that are often used by persons with malicious intent. The focus is on finding security weaknesses in target environments that could let a potential attacker penetrate the network or computer systems and identifying zero-day exploits. Attempts are made to compromise target systems and ultimately to steal information. This typically requires tools and techniques very similar to those that a malicious attacker would use. Testing methodologies address the introduction of new methods of code analysis, which mirror those attacking a system.

Review Execution and Planning

Coordination of an integrated testing and reporting schedule for a 12-month period occurs typically. The coordination of these tests reduces inefficiencies caused by disjoint attempts at having engineers plan reviews and frees up technical staff to focus on security issues. Technical Writer assists in the development of reporting. This approach ensures a quality and a uniform reporting product that is readily useable by a customer.

Surge Methodology

Proper scheduling and preparation of security assessments greatly reduce the amount of surge support needed for application security testing by creating a more well-coordinated operating environment. However, in the event that surge support is needed to increase the number of initially scheduled reviews, additional security personnel are made available on an as-needed basis.

Routine Vulnerability Scanning

Vulnerability scanning of program objects is conducted routinely.

Enhanced Assessment Capabilities

After customer review of a proposed augmentations to the existing vulnerability – scanning infrastructure, a plan is submitted to implement accepted recommendations. This includes the implementation and procedures to conduct routine, operational, and transitional assessments across an enterprise.

Password Cracking

Password-cracking exercises are conducted on common enterprise infrastructure products using commercial tools. The results are documented and delivered to the Continuous Monitoring Manager.

Vulnerability Tracking

A full operational vulnerability tracking database is implemented as part of the COTS Enterprise Security Portal (based on Microsoft SharePoint) used to monitor and report on all security tasks. This portal not only reports all relevant information for the tracking of vulnerabilities, it also contain peripherally related security information and supports the creation of custom reports.

Vulnerability Notifications

A Security Enterprise Portal includes automated mechanisms for distributing vulnerability information via email system and notifications when security managers login to the portal.

Vulnerability Remediation

The closure of vulnerabilities is facilitated by working with system points-of-contact to determine a course of action for remediation, assisting in scheduling the remediation activity, and verifying that the vulnerability has been dealt with. Information regarding the remediation plan of action, scheduled remediation activity, contact information, and the current status of the vulnerability are presented via the Enterprise Security Portal.