LESSONS LEARNED FROM IMPLEMENTING RISK MANAGEMENT FOR A LEGACY SYSTEM

Col (Select) Rakesh Dewan
USAF - ICBM System Program Office
ICBM Integration Contract Program Manager
Building 1258, Hill AFB, Utah 84056
801-777-9159, Fax: 801-775-2194
rocky.dewan@hill.af.mil

Mr. David Lindblad
TRW - ICBM Prime Integration Contract
Assessment and Risk Management Integration
888 S. 2000 E., Clearfield, Utah 84015
801-525-3473, Fax: 801-525-3440
david.lindblad@trw.com

"Program management is risk management!" *- Unknown.*

ABSTRACT

Implementing the risk management process is an art coupled with science. Much has been written on the "how to" and "advantages" of implementing the process for new programs. However, there is a void in the literature describing the advantages of implementing the process for legacy systems. This paper shares the successes, challenges, and lessons learned during four decades of successfully implementing and formally embracing the risk management process for an Air Force legacy system--the Intercontinental Ballistic Missile (ICBM) weapon system.

The ICBM Team includes members from all related government and contractor organizations. The primary objective of the team is to sustain the weapon system through 2020. One of the main reasons the team has been so successful in maintaining the legacy system is their successful implementation of the ICBM risk management process. This process has been tailored and fine-tuned as appropriate for a fielded system to ensure that the ICBM system remains the vanguard strategic deterrent system.

BACKGROUND

The ICBM system was first deployed in the 1960s and currently consists of 500 Minuteman III and 50 Peacekeeper strategic missiles. The total ICBM force provides the nation with an extremely cost-effective means of continuous strategic deterrence. The system includes hardware, software, infrastructure, and well-established processes, many of which are decades old.

Appendix A provides a brief description of the current ICBM hardware and function. Appendix B provides a background of ICBM system management from a risk management perspective. It includes a discussion about the recent transition of Total System Performance Responsibility (TSPR) from the Air Force (AF) to a Prime Integration Contract and attendant risk management implications.

RISK MANAGEMENT CHALLENGES

The overarching ICBM risk management challenges include:

- Sustain ICBM system capability at or above requirements through 2020.
- Provide accurate and timely estimates of current and projected component, subsystem, and system capability under a variety of scenarios useful for managing the system.
- Predict or detect degradation with sufficient lead-time to mitigate the degradation before impacts to system functions are realized.
- Determine feasible and best value mitigation options to meet requirements while meeting challenges related to diminishing supplier availability.
- Mitigate impact to system function by repairing or replacing degraded hardware before system degradation.

NEW/YOUNG SYSTEM VERSUS LEGACY SYSTEM

In a new system, risk management focus is on the design, manufacture, and deployment risks,

including mitigation of latent defects, related to meeting requirements. Modifications of component, subsystem, and system requirements of a new system may sometimes be allowed to mitigate technical, schedule, and cost risks or to implement the "Faster, Better, Smarter" philosophy (best value determination). Other solutions such as design changes, manufacturing process changes, and material changes may also be used to mitigate risks as they arise.

On the other hand, a legacy system has risk management challenges that encompass the entire spectrum of development, deployment, and sustainment of new and old subsystems together while ensuring that the new components that replace worn out, failed, or obsolete components also meet requirements. Figure 1 illustrates the risk challenges the team faces each day to sustain the ICBM legacy system.

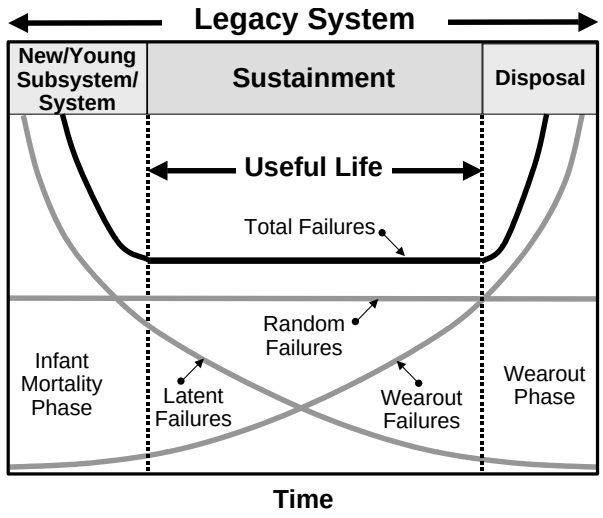

Figure 1. New System versus Legacy System

When the legacy system deploys new components to mitigate degradation due to wear-out trends of old components, it encounters risks similar to those of new systems. However, unlike a new system, the legacy system does not have all the risk mitigation options that are available to a new system. For example, a legacy system does not have the luxury of total redesign when only a single subsystem exhibits degradation. Unlike requirements of a new system in the development phase, the form, fit, and function requirements for legacy system components are not negotiable and cannot change. Any change to the functional or physical specification of a component could have major impacts to the system, a risk that is totally unacceptable to the team. In addition, there are risks associated with replacing degrading components with new components in time to continue to meet requirements without impacting performance of other components, subsystems, or the system. The team identifies these risks by increasing the monitoring and analysis of both older and newly deployed components.

RISK MANAGEMENT CHALLENGES UNIQUE TO A LEGACY SYSTEM

There are unique risk management challenges with sustaining a legacy system in order to meet or exceed established component, subsystem, and system requirements. These include:

- Detect or preferably predict with high certainty, wear-out degradation early enough to deploy new or refurbished replacements before system impact.
- Manage risks related to components that are exceeding their useful life.
- Simultaneously manage risks related to new component development and production, and those related to component refurbishment, to replace degrading hardware.
- Manage integration of new technology with old technology that is decades old.
- Determine solutions to handle the loss of qualified vendors and the loss of trained and certified personnel while replacing degrading components that must continue to meet original form, fit, and function requirements.
- Maintain decades old manufacturing processes and documentation.
- Maintain vigilance by isolating latent failures from random and wear-out failures so new component design and processes can be updated.

- Meet increasing environmental, safety, and security requirements while integrating new and older components and processes.
- Maintain high confidence that all requirements are being met while integrating new components with older components.

LESSONS LEARNED

In addressing problems on a daily basis, the team continues to successfully blend the right mixture of risk management art and science to sustain the system without compromising requirements. In the decades of conducting risk management for the legacy ICBM system, two categories of lessons learned were identified:

- Lessons learned common to all program phases including development, production, and sustainment phases.
- Lessons learned that are unique to the sustainment phase of a legacy system.

LESSONS LEARNED THAT ARE COMMON TO ALL PROGRAM PHASES

KEEP THE RISK MANAGEMENT PROCESS IMPLEMENTATION SIMPLE!

Keep the process implementation simple. It is clear that the best risk process implementations are those that are easy to understand, easy to explain to others, and are easy to implement while meeting the needs and requirements of the team to successfully manage risks. The team cannot consistently comply with the implementation if it is too complicated. Complicating any part of the implementation will increase the chance of costly mistakes or system failure that may be realized from risks that are not properly identified, assessed objectively, prioritized properly, and mitigated. In addition, training costs increase rapidly as the process becomes more complicated. Most importantly, a complicated implementation takes focus away from managing the risks. Those that disagree with any aspect of a complicated implementation will be right there to remind you about how complicated it is. So, keep it simple!

Keep the ground rules simple. The ground rules for identifying, evaluating, tracking, and reporting risks must be clear and easy to understand for every team member at every level.

Keep the products simple and standardized. The easier it is for the team to create and understand the products, the better. Software that is straightforward to use and templates that are easy to fill-out enhance the risk management activities of the team. When products are kept simple with a standard recognizable format, the team can more easily and objectively evaluate, prioritize, track, report, and mitigate risks.

Keep the tools simple. "Expensive" does not necessarily mean "Better" when it comes to risk management tools. If every member of the team is required to read complicated and lengthy tool manuals to create products, then the tools may not be worth the effort. Commercial-off-the-shelf software already being used by the team in other day-to-day tasks will work just fine. This kind of software is available, relatively inexpensive, easy to use, well-documented, and very flexible for quick and simple product creation and improvement. Low cost technical support and updates are also generally available for this kind of software. If the team is connected via network, then this task is even easier.

Keep documentation simple. If the process, products, and tools are kept simple and accessible, then the documentation will be easier to keep simple, complete, accessible, consistent, and current. This will allow the team member with the least experience with the process to understand the documentation thereby increasing the chance for successful and objective implementation.

[Note: Italicized text describes the ICBM team's actual experiences and/or solutions related to the lessons learned.]

The ICBM team researched several risk management tools and products. We now use a tailored set of products designed to fit our

needs. We use a very simple reporting and documentation process. We have standardized products with templates using commercial-off-the-shelf spreadsheet, chart, and schedule creation software common and available to all team members. We also explain the templates, ground rules, and all other aspects of implementing the process in an online tutorial available to every team member. The documentation is routinely updated on a monthly basis, or more often if necessary. In addition, we hold process meetings to regularly remind ourselves about keeping the implementation simple whenever we consider potential product improvements. Currently, the entire team (customer, program office, ICBM prime contractor, and other related contractors) uses a single streamlined documented process to manage risks.

REQUIRE CONTINUOUS MANAGEMENT COMMITMENT

Managers must "Walk-the-Talk." Senior Managers (and all managers) from all participating organizations must be committed to designing a simple standardized risk management system, and they must use it! Leadership commitment must be demonstrated every day. They must "Walk-the-Talk" and not just "Talk-the-Talk" or implementation will be sporadic resulting in major technical, schedule, and cost impacts. For example, managers must encourage risk identification, objective risk assessment, and objective status reporting or risks may be misprioritized or go unnoticed until realized by costly errors or system failure.

Managers must provide resources to do the job. Managers must provide sufficient and appropriate resources including qualified personnel, training, tools, and environment. Managers must set priorities to allow time to properly conduct risk management. Managers must also provide sufficient funds to mitigate risks.

Managers must provide positive influence. Management must not just be committed and provide resources. They must support, defend, and use the risk management products. Workers will follow their lead; any waiver at the top will set ripples in motion that may take a long time to smooth out.

Managers must encourage risk identification and objective reporting on risk status. Managers must instill in their teams that it is "OK" to identify risks and quickly bring them forward as soon as possible--don't shoot the messenger! They must encourage teams to continue surfacing issues early, no matter how negative the news may be. Managers must also encourage the team to objectively report risk status so that objective risk management decisions can be made. If the team feels threatened, then they will resist, risks will be overlooked, and program impacts may occur. It is far better to evaluate a large list of risks to determine which must be mitigated than to sift through an incomplete list.

Managers must use the risk management products in decision making. Managers must be committed to using the risk management products in order to make critical and objective programmatic decisions.

Managers must accept the importance of risk management. Managers must go beyond thinking that the process only adds value for new or large development programs and is not applicable to all programs (including a legacy system program). Risk management should be the most important job of all program managers--"Risk management *is* program management." If managers do not see that a robust risk management system will have a direct impact to their bottom line--operational impact or profit impact--then, they may have a tendency to put in their "C-Team" versus their "A-Team" to work risk issues. It is the responsibility of the entire team to demonstrate the importance of implementing risk management.

Our risk management process implementation is successful because management walks the talk. The ICBM risk management process is the common communication and management tool used by every member of the ICBM team--from the senior managers to the first line supervisors of both the government and contractors.

DESIGN AND STANDARDIZE RISK MANAGEMENT IMPLEMENTATION

Design an implementation that follows the basic process. The team must follow a basic risk management process. A basic process, such as the one illustrated in Figure 2, is simple, well understood, and widely accepted. Although the basic flow is simple, there is not yet an all-encompassing process implementation design, there are many variations.

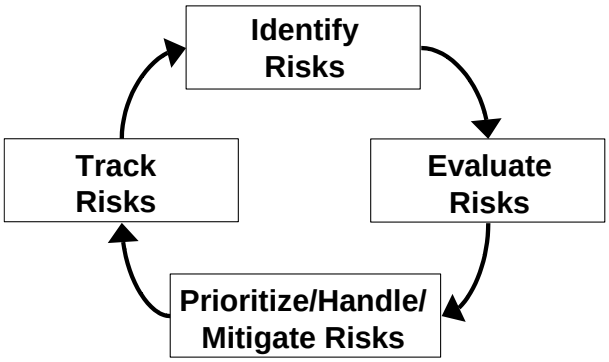

Figure 2. Basic Risk Management Process

Tailor the design. Invest resources to design a simple, accurate, thorough, and concise implementation tailored to meet program requirements and needs, while following the basic process. Involve a variety of team members with the design development (including contractor and government organizations) to improve the design and to help gain commitment in the implementation of the design.

Standardize the design. Standardize the design to assure that risks are objectively evaluated and risk management decisions can be made objectively. A standardized design is easier for the team to understand and implement uniformly.

Standardize the risk evaluation guidelines. The set of evaluation guidelines includes tables of decision intervals used to assign technical, schedule, and cost risks as high, medium, or low probability and impact. Additional guidelines may be needed for determining when a subprogram risk should be considered as also having impact to the overall program or to another subprogram. In this case, the risk may be dual-monitored by all subprograms affected by the risk and by a system integration team.

Standardize the risk management products. Standardize the set of products to make it easier to understand and create those products. Help minimize information gaps by requiring that all entries in each product be filled. Standardize the products to streamline critical information to the team when making risk management decisions and to help the team remain objective, focusing on managing risks rather than on understanding a disjointed set of products.

Document the design. Document the design with enough details so there is no guessing about risk evaluation and reporting formats. The documentation must help train the team to ensure that risk evaluations and products remain standardized.

Coordinate the design. Coordinate the documentation with the team to ensure the design meets all program needs and requirements.

Maintain the design documentation. Update the documentation periodically as value-added improvements are made. Notify the team of the updates to ensure continued standardization.

The ICBM team invested considerable time to streamline the risk management process and developed a common set of process documentation that meets the program management needs of the team.

The ICBM team products are standardized and include:

- *Risk evaluation forms, which contain details about each risk including description, points of contact, quantified risk evaluation in terms of probability and impact, and a summary of the risk mitigation or handling plan.*
- *Risk management watchlists, which are spreadsheets of all the risks including description, probability and impact summary, major changes to each risk since the previous reporting period, and a status summary stoplight color*
- *Risk management watchlist summaries, which*

are tables of top-level summary information that include the number of risk items, mitigation status summaries, and a list of major changes since the last reporting period

- *Risk quantification projection graphs, which are charts of potential component, subsystem, or system capability versus year, with and without mitigation*
- *Detailed risk mitigation plans and schedules*
- *Risk Management Data Book, which is published monthly and includes the risk evaluation forms, watchlists, and watchlist summaries*

The ICBM team documentation includes:

- *Contractual references to risk management*
- *Risk management objectives*
- *Point of contacts list*
- *Definitions and acronyms list*
- *Process implementation flow*
- *Simple list of steps for identifying risks so every team member can identify risks and bring them into the system*
- *Risk evaluation guidelines*
- *Templates for the products, instructions for creating the products, examples of completed products, and the list of software tools to be used to create the products*
- *List of periodic meetings where risk management is a topic that includes meeting dates, agendas, and a list of products to be prepared and presented at each meeting*
- *Documentation in the Integrated Master Plan of other processes that provide input to, or receive input from, the risk management process*

CONSIDER PROCESS IMPLEMENTATION IMPROVEMENTS

Evaluate and screen potential changes. The implementation of the risk management process must be continuously evaluated and assessed for potential improvements. When the design is first implemented, it may need to be improved. As the implementation matures, changes will likely decrease. Process implementation can always be improved (continuous process improvement). All suggestions should be evaluated and screened. However, some changes suggested because of process misunderstandings can be simply avoided by training or by improving the documentation. Implementing too many changes all at once may cause negative results due to combination effects among the changes not anticipated until implementation proceeds. In addition, some suggestions may at first seem insignificant but may instead cause significant and unnecessary negative impact. For example, changes that require all risks to be completely reevaluated, but add no significant value, should be avoided. To save time, suggested changes may be compared to a list of previously rejected changes. Screened changes are then brought forward to the team for coordination and implementation. Every change must pass the "Keep it simple!" test. On the other hand, spending too much time trying to improve the process by frequently implementing many process improvement changes is a negative distraction and adds confusion. This will distract focus from risk management to process management. It may be best to simply focus on implementing the subset of improvements that add the most value.

The ICBM team has an "open mind" policy when it comes to improving any process. Any member of the team can recommend improvements to the risk management process and the risk management integrator logs in all inputs. The suggestions are reviewed and feedback is provided to originators on the disposition of their suggestions. To date, coordinated and implemented improvements have ensured that the process and products are kept as simple and streamlined as possible to meet the current and future needs of the ICBM program.

PROVIDE TRAINING

Create a training document. Develop an easy to understand, concise, thorough, and accurate tutorial that is accessible to every member of the

team. This can be achieved with a computer-based tutorial. The tutorial should highlight senior management support for the program and the importance of the team in implementing the process.

Hold training sessions. It is critical to train all team members to be fully qualified to implement the process from the start. Once initial training has been provided, an additional refresher is always available via computer-based training. The training is not a one-time exercise. The team must be kept informed with timely notification of process improvements and product updates.

The ICBM team is committed to training. It added ICBM risk management training to new employee orientation and program management training courses. All the current and complete process documentation and training material are available on the team's intranet for new team members to review or others to reference.

MAINTAIN OPEN AND CONTINUOUS COMMUNICATION

Communication is the risk management lifeline. Communication holds the risk management process together and is required to cost effectively mitigate risks and manage programs. Examples of how to improve risk management communication are as follows:

Hold regular risk management meetings. Plan and hold regular meetings with the entire team. Make the meetings a meaningful habit. Meeting topics include risk identification, evaluation, handling, prioritization, status, and mitigation funding requirements all displayed using standard products. The frequency and content of the meetings must be tailored to fit program needs. Publish meeting agendas in advance to ensure that meeting purposes are clear to all and to allow the team to prepare. Allow ample time for discussion and understanding, but do not tolerate hidden agendas or entertain motions for changing the process at risk management meetings. As stated earlier, management commitment is required, so it is imperative that senior leadership (both government and contractor) chair risk meetings. For example, the chief engineer for the government and the senior engineering manager for the contractor may co-chair risk management board meetings held prior to each program management review.

Hold risk management processes implementation meetings. The purpose of these meetings is to discuss potential process improvements, implementation issues, and discrepancies. Major process changes should be coordinated with team leaders at the process meetings. Process meetings must be separated from risk management meetings so the risk management meetings can focus on managing risks.

Maintain an action item list. As external issues arise, the chair of the risk meetings should place them in a parking lot and assign action items to the proper team members. If a process issue is brought up at a risk management meeting, then it should be transferred and discussed at a process meeting. Assure team members that their issues are important and will be resolved by statusing each action item at the beginning of each meeting and by confirming the new action items at the end of each meeting.

Make the documentation and products accessible. Require an open-file policy for the team when it comes to accessing the risk management products. Keep all the latest information accessible to help keep communication lines open. Ensure that the team has easy access to current products to allow them to continue using the products designed to help them make risk management decisions.

The ICBM Team holds monthly risk management board meetings and holds process meetings as required. The team noticed a significant change in focus to managing risks at the board meetings the moment it was decided to stop discussing the process at those meetings and begin taking action items to discuss it at the separate risk management process meetings. In addition, the team maintains a current set of risk management products on the team's intranet to keep all team members well

informed.

FOLLOW THE PROCESS

Once the approved risk system is implemented, it must be followed. Do not accept the syndrome of: "We don't have time to do it right, but we have time to do it over." If people stray from the approved system, then risks may be overlooked or at best be prioritized improperly. The entire team must be vigilant and follow the process!

PAY ATTENTION TO THE LESSONS LEARNED FROM OTHERS

Research and apply lessons learned. Pay attention to lessons learned from others. This is the single most effective method for streamlining the design and successful implementation of the process. Do not try to re-invent the wheel. Lessons learned can be found from literature searches, risk management forums, and from inquiries about the experiences and knowledge of others. Lessons learned should be captured and stored. In addition, it is a good idea to capture information about risk items as they are opened, closed, or changed for future reference.

Periodically review the list of lessons learned. Capture all the lessons learned in a database, including the list of all closed risk items, which should be reviewed periodically to determine current applicability.

The ICBM Team maintains and periodically evaluates our lessons learned file. The team also researches lessons learned from others and sends team members to risk management forums to keep the process implementation current and free of problems.

LESSONS LEARNED UNIQUE TO A LEGACY SYSTEM

Although this section relates generally to any legacy system, much of it is specific with examples related to the ICBM program. Thus, the italicized text format used in the previous section is not included.

DESIGN AND IMPLEMENT AN ASSESSMENT PROCESS

Conduct assessment to provide early warning of potential degradation. Proper assessment of component, subsystem, and system capability is required to provide early warning of potential degradation to system capability. The assessment process includes testing and monitoring of component, subsystem, and system level hardware. The test and monitor data is archived and assessed to identify changes and predict impacts to system capability, if any. Potential impacts must be identified with sufficient lead-time to allow the team to develop mitigation plans, obtain mitigation funding, and execute the plans before negative system impact. The job does not end there. If degrading components are repaired or replaced with new components, then the team must assess the newly deployed components along with existing hardware to ensure there are no new trends or impacts.

Determine assessment process objectives. The objectives of the ICBM assessment process are to:

- Identify degradation and distinguish between latent, random, and wear-out failures.
- Provide accurate and timely estimates of current and projected capability under a variety of corrective action options that are useful for managing the system.

The importance of early warning (prediction or detection) of potential degradation to implement corrective action to maintain system capability is illustrated in Figure 3. The figure illustrates how early detection of degradation with consequent timely mitigation (corrective action) maintains capability above acceptable levels.

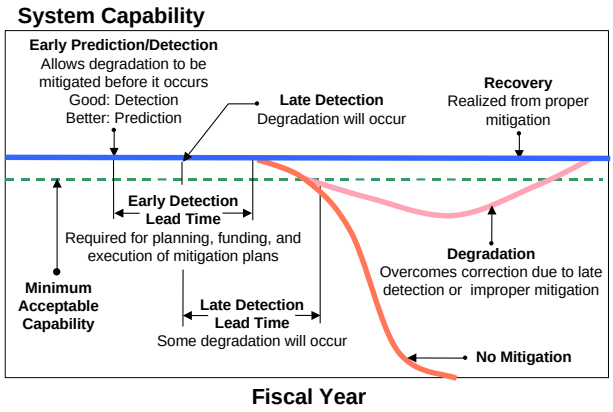

Figure 3. Degradation and Recovery

Design and implement the assessment process. The process must be tailored to fit the needs of the individual program. The details of the ICBM assessment process are documented in References 1 and 2. The process outline is:

- Conduct requirements analysis to determine component, subsystem, and system requirements.
- Conduct failure modes and effects analysis to determine hardware failure modes and mission criticality.
- Conduct age sensitivity item analysis (ASIA) to establish the list of age-sensitive mission critical components to be periodically tested to identify aging trends.
- Establish the set of critical parameters and limits (failure limits or distributions, margin of safety limits, etc) by which component, subsystem, and system capability will be tested or monitored.
- Determine test and monitor requirements. Identify gaps in data, determine number of items to be tested periodically to build statistical confidence in detecting changes.
- Collect, store, and manage the test and monitor data. Obtain data from sources such as from operational tests, ground tests, lab tests, visual inspections, field performance records, and maintenance and repair records. Establish the historical database baseline set to be used for comparison to detect changes. Make the data accessible for analysis.
- Conduct analysis to identify trends, assets shortages, and other problems. For example, determine statistical correlations, predict trends or other changes, investigate component subpopulations, and determine component age distributions.
- Validate data and analysis, and flag trends. For example, validate test data, assumptions, failure modes, and failure limits. Flag the trends to the team.
- Identify impacts. Determine potential component, subsystem, and system capability impacts. For comparison, make capability projections with and without mitigation.
- Conduct trade studies using the projection comparisons to identify and quantify mitigation options so informed risk mitigation options and decisions can be made.

Implement an Aging Surveillance process. An aging surveillance process is included in the assessment process but focuses on aging or wear-out trends.

USE THE ASSESSMENT PROCESS TO IDENTIFY AND QUANTIFY RISKS

Integrate the assessment and risk management processes. Figure 4 illustrates how results and products from the assessment process, such as trend identification and capability projections, are input to the risk management process. These inputs are used to develop and implement plans to mitigate degradation.

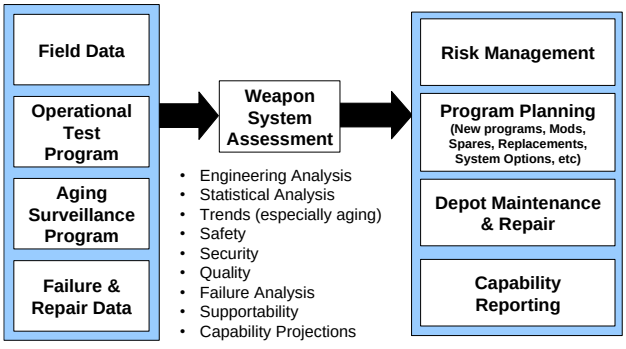

Figure 4. Integration of the Assessment and Risk Management Processes

Quantify capability projections--with and without risk mitigation. Quantify capability projections to help determine risk mitigation options and priorities. Some risks may be related to component degradation of key performance parameters due to wear-out or use. Key performance parameters are measures of capability and may include availability, reliability, accuracy, and survivability. Risks affecting capability are modeled at the component, subsystem, and system level and projections are quantified as illustrated in Figure 5. Risks related to component shortages, such as due to wear-out or use, are quantified as illustrated in Figure 6. If a component is mission critical, then system availability projections may be a function of component asset quantity projections. All data, models, assumptions, and projections must be readily available to the team so mitigation options and priorities can be properly assessed.

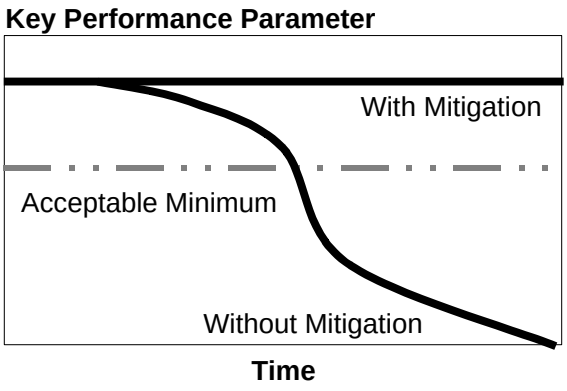

Figure 5. Capability Projection

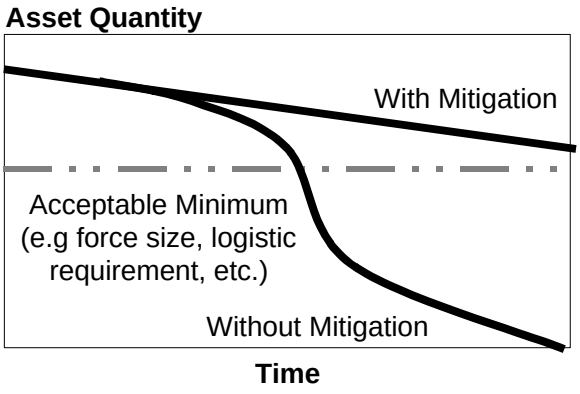

Figure 6. Component Asset Quantity Projection

INTEGRATE MITIGATION PROGRAM RISKS AT THE SYSTEM LEVEL

Risk management must be integrated at the system level and between all related programs. Once risk mitigation priorities are made, subprograms must be implemented to mitigate the risks. The risk process must also be implemented for each of the subprograms. Some subprogram risks are managed only within each subprogram. However, risks must be integrated if risks from one subprogram affect another subprogram. The subprogram teams and the system integration team must all pay close attention to those risks.

MEET CHANGING ENVIRONMENTAL, SAFETY, AND SECURITY REQUIREMENTS

Another risk management challenge of a legacy system is to maintain the system in times of austere budgets, while ensuring that the customer is delivered the best value product. Replacement parts can cost many times more than their original cost because of loss of qualified vendors, challenges of maintaining original technology while the world is moving to throw away technology, and the requirements to use only environmentally friendly materials. For example, a replacement for Freon, once used in the liquid injectant thrust vector control of the Minuteman Stage 2 motor, had to be found and qualified to ensure that it met or exceeded the requirements of the original Freon.

It is also becoming more difficult to obtain support for decades old manufacturing and repair processes. This is especially true when some were not well documented or changes that were implemented on the factory floor were not adequately captured. It is difficult to replace old degrading parts because they must have the same functional and physical characteristic as the old parts they are replacing.

The redesign task is further complicated by the requirement for nuclear surety and system safety. No compromise shall be allowed on the nuclear safety record of the ICBM strategic force--Zero Tolerance.

MEET CHALLENGES OF THE LOSS OF VENDOR BASE AND QUALIFIED/CERTIFIED PERSONNEL

The consolidation and loss of qualified/certified vendor base for manufacture and repair and the loss of qualified/certified personnel are major risk challenges for a legacy system. These risks also increase as the baby boomers reach retirement age. These are very real concerns given the great number of consolidations that have occurred in the defense industry due to the peace dividend. According to "The Distillation of the Defense Industry" (Reference 3), the defense industry is "shrinking with dizzying speed as Pentagon budgets plummet and contractors either merge or team up to compete for the few remaining US procurement programs". In one example, a large corporation merged together twelve separate entities. The reference also states that the industry has lost more than two million workers.

MAINTAIN LEGACY DOCUMENTATION

Capture documentation. The team must capture all the as-build design data of each component. This documentation includes such things as manufacturer build records, manufacturing processes, and material formulations. This documentation can help the team isolate latent failures and future wear-out failures that must be mitigated to sustain the system. History has shown that program teams concentrate on design, development, and fielding far more than they do on documentation. Thus, the manufacturing and material processes of legacy systems are usually incomplete. Although the documentation may not fully capture all the data needs of the program, there is critical design documentation that are of value to maintaining a legacy system.

Store documentation. The team must store complete, accurate, and current development or redesign data. The team may consider using electronic means to scan and store these potentially invaluable data for easy data access in the future and to prevent data deterioration.

Use the documentation. As previously mentioned, if the documentation is captured and stored, then it can be used to isolate and mitigate latent and wear-out failures to sustain the system. In addition, as personnel change, the documentation helps in training, troubleshooting, and redevelopment when a component needs to be replaced or upgraded.

Plan and budget for documentation. Program managers should focus on the value of capturing accurate and complete documentation to avoid risks in the future. They should plan and set aside sufficient budget for the documentation early in the program.

THE FUTURE

The ICBM team is embarked on simplifying, standardizing, and improving the team's implementation of the risk management process to sustain the ICBM weapon system well into the future.

Risk charts are now being improved and standardized to include quantified impacts to the system if mitigation efforts are not approved and funded, and to include the cost associated with risk impacts and mitigations. These charts provide the decision-makers with the information needed to understand the impacts if it is decided to place a low priority on a mitigation effort. Risk charts are also being improved to include assessment of risks associated with budgeting of all risk mitigation efforts.

All personnel are being trained, especially those not experienced in formally implementing the risk management process. As a result, they become converts to the implementation that helps them improve their program management skills.

The continued success of the team's implementation of the process has enlightened members on it's value to not only manage risks, but to also quantify and defend risk mitigation budgets. Each member of the team is encouraged to keep the communication lines open by providing all the data they have available and to present their case to the risk management board.

The success of ICBM team's implementation of the risk management process is instilling confidence in the team because it helps the team make smarter and more objective and timely risk management decisions to meet the requirements of the legacy ICBM system.

The team continues to insure that we meet the "4-Cs" of the ICBM risk management process implementation--Commitment, Communication, Cooperation, and Continuous "value added" improvement.

In conclusion, program management and risk management are two edges of the same sword and one cannot exist without the other. To say it another way:

"Risk management <u>is</u> program management!"

REFERENCES

1. <u>Prime Integration Contract Integrated Master Plan</u>, Contract F42610-98-C-0001, 3 November 1999.
2. <u>ICBM Weapon System Assessment Process</u>, process description document, TRW, October 1997.
3. <u>The Distillation of the Defense Industry</u>, John A. Tirpak, Air Force Magazine, July 1998.

APPENDIX A
THE ICBM WEAPON SYSTEM
PHYSICAL DESCRIPTION

The Minuteman III and Peacekeeper systems each consist of a three-stage solid propellant booster, a liquid propellant post-boost propulsion system, an inertial guidance system, and a nuclear reentry system with a range of over six-thousand nautical miles. The Minuteman III missile is 59.9 feet tall, 5.5 feet in diameter, weighs 79,000 pounds, and has a payload of up to three reentry vehicles. The Peacekeeper missile is 71 feet tall, 7.7 feet in diameter, weighs 195,000 pounds, and has a payload of up to ten reentry vehicles. The system infrastructure includes the launch facilities, missile alert facilities, Hill Air Force Base depot, missile and motor transportation and handling equipment, contractor build facilities, contractor and AF test facilities, and material and component vendor facilities.

Minuteman III

Peacekeeper

Infrastructure

APPENDIX B
ICBM WEAPON SYSTEM
BACKGROUND FROM A RISK MANAGEMENT PERSPECTIVE

The ICBM weapon system is one leg of a nuclear triad (the other two legs of the triad are bombers and submarines) that provides the United States with an extremely cost effective means of continuous strategic deterrence.

The ICBM system was originally deployed in the late 1960s. The current system consists of the Minuteman III and Peacekeeper nuclear weapon systems. The Minuteman system is the older of the two and was originally deployed in the early 1970s, while Peacekeeper was deployed in the late 1980s. The original design of both systems called for a service life goal of approximately ten years. However, due to fiscal and political constraints, the systems were kept in service well past their original design goals.

The current policy calls for performing life extension upgrades to the major critical systems so that the ICBM system will continue to meet the strategic needs of the nation well into this century. Given this policy, the ICBM team is required to sustain all the hardware, software, infrastructure, and processes related to both the Minuteman and Peacekeeper systems. Current plans call for sustaining the Minuteman system until 2020, and sustaining the Peacekeeper system as directed by the senior leadership.

These systems are in a high state of maturity and are therefore in the sustainment portion of their life cycles. Sustainment consists of assessing component, subsystem, and system performance, repairing or building new hardware and software, improving processes, and buying goods and services to maintain the systems. The team identifies wear-out trends that could impact system performance with sufficient lead-time to allow the ICBM program office to plan and budget for the fixes.

During the early stages of development, the government decided the best approach was to have the government take on the Total System Performance Responsibility (TSPR) and the risks associated with it. Consequently, the AF, assisted by TRW Corporation as the System Engineering and Technical Assistance (SE/TA) contractor, was given TSPR over the land-based ICBM system. In this role, the AF, assisted by TRW, was the system developer and integrator and directly contracted on a competitive basis with industry to produce the system and the infrastructure while retaining overall program integration and management responsibilities and risks.

The ICBM team program and processes have evolved. For comparison, the sections below describe how the team managed the program and associated risks before 1998, and how the team is now managing the program and has shifted TSPR to a Prime Contractor.

PRE-1998

From the 1960s through most of the 1990s, the AF, assisted by TRW, was the ICBM system developer and integrator. The team worked with 100 plus contractors to design, develop, produce, field, and sustain the ICBM system.

In the early years of the ICBM program development the AF assembled a government and contractor team that would be willing to push the envelope of project management, technology, system design and integration to the maximum. Due to the Cold War, the AF had great political support for the ICBM strategic deterrence weapon system. Thus, the political leadership provided considerable resources and the program was on a fast track. During the early years, formal and structured program management and risk management processes were just evolving. The ICBM program risk management methodologies used in the early years were not always uniform. Since the program goals were to deliver a reliable system on time, and the team had access to an abundance of resources, each contractor was allowed leeway to deliver a design that met the program requirements. Therefore, the AF and SE/TA team worked with the individual

contractors to understand their management approach. Another reason there was not a robust risk management process implemented at that time was because the team had the resources to implement a parallel development approach. If they ran into a problem, they provided addition resources to eliminate it or develop a new approach.

This approach worked well but had impacts as the decades progressed. As the team grew, and as the program management and risk management processes matured, the 100 plus contractors refined their management efforts to fit their corporate circumstances--Defense versus Commercial. During this time, the AF and SE/TA team was also refining their system development and integration capabilities as well as their system program management skills--including risk management. Thus, in the 1970s through the 1990s the team focused on having a robust risk management process versus forcing the team to adapt to a standardized or single risk management process. This philosophy served the ICBM team--AF, SE/TA, and Associate contractors--well into the 1990s. Nevertheless, when the Berlin Wall fell, the nation was demanding a peace dividend. The ICBM team soon learned that as the industrial base dwindled, and the resources became scarce, the team could not continue to operate in the same way. In addition, both of the ICBM systems were fast approaching their life cycle age-out goals.

POST-1998

In 1996, the senior leadership of the AF made a decision to employ a Prime contract concept to the ICBM program versus managing the 100 plus contracts. The AF, after evaluating all options, determined that the Prime Integration Contract concept offered considerable advantages over the old way of doing business. Thus, the ICBM program office was authorized to conduct an open competition for selecting a best value Prime Integration Contract team that would be given TSPR over the ICBM system. The ICBM program office worked with industry and competitively selected the ICBM Prime Integration Contract team headed by TRW Corporation. The team was awarded a basic contract in 1998 valued at over three billion dollars. It consisted of a basic contract with fourteen annual options to sustain the ICBM system through the year 2012.

One main area of interest for the AF during the best value consideration of a Prime contractor was how the Prime would manage the effort including identifying and managing the total program risk under TSPR. TRW Corporation had outlined a robust risk management process, which included a single overarching process for the entire team to follow. The process was implemented as described in this paper and has been refined as needed to meet the needs of the program.