

Risk Management Experience on Hyperion

Edmund H. Conrow, Ph.D., CMC, CPCM, PMP, Consultant
Stephen L. Carman, TRW Space and Technology Division

Introduction

This paper briefly describes the application of risk management to the Hyperion project, a complex electro-optical instrument developed by TRW for NASA Goddard Space Flight Center (GSFC). The very short schedule, coupled with substantial technical development activity and tight budget, made Hyperion a relatively high-risk project. Yet the application of an aggressive risk management process described here contributed to Hyperion being delivered slightly ahead of schedule, meeting all performance requirements, and within budget. This risk management process, along with the resulting lessons learned, is applicable to a wide variety of commercial, government, and defense projects.

Programmatic and Technical Background

The Hyperion instrument provides a new class of earth observation data for improved Earth surface characterization. Hyperion is a complex hyperspectral spaceborne imager that provides a pushbroom-type image of the earth's surface with 30-meter spatial resolution over a 7.5 km swath and 220 contiguous spectral channels from 0.4 to 2.5 microns in wavelength. Spectral bandwidth of each channel is 10 nm. The instrument uses two focal plane arrays (FPAs), a visible near infrared (VNIR) and a short wavelength infrared (SWIR). The SWIR FPA is actively cryo-cooled to 110 K using a pulse tube cooler. The unit is self-calibrating and will use the sun and moon for additional calibration sources.

The Hyperion project was conceived by NASA GSFC to solve a problem they encountered in the development of the Earth Observer One (EO-1) spacecraft, the first of the earth-observing missions in their New Millennium Program. The problem occurred when the grating imaging spectrometer (GIS) and wedge imaging spectrometer (WIS) could not be completed as planned, and NASA terminated the contracts. This left a hole in their planned scientific validation of the Advanced Land Imager (ALI).

TRW Space and Technology Division had delivered a similar hyperspectral imager for a previous mission (Lewis), and spare hardware from that development project was proposed as the basis for quickly fabricating a replacement for the GIS. NASA agreed with the idea, but required the instrument to be completed in less than half the time that would normally be required for such a development (12 versus 24 months).

To complicate matters, the scope of the project grew as a result of studies of the steps required to disassemble ALI and the spacecraft to integrate Hyperion late in the spacecraft assembly and test schedule, which would require so much time that it threatened the scheduled launch date for the EO-1 spacecraft. Instead, it was agreed that Hyperion should be designed as an independent instrument rather than integrated into the ALI, as had been planned for the original GIS. This meant adding a telescope and the associated motorized aperture door, and the supporting structure. Now a significantly more complex instrument had to be built *in the same 12 months*.

Fortunately, spare telescope hardware from other instruments was available at the subcontractor (SSG) to expedite delivery of the telescope and spectrometer opto-mechanical subsystem. This delivery and a lot of hard work enabled Hyperion to be delivered a week *ahead* of schedule.

But the early Hyperion delivery would not have happened without the use of a comprehensive risk management process—this was a major factor contributing to the success of the project. In fact, NASA had insisted on a rigorous risk management process because they felt that poor risk management had led to the failure of the previous WIS and GIS projects.

Hyperion Risk Management Process

The risk management process implemented on Hyperion was composed of risk planning, risk assessment (identification and analysis), risk handling, and risk monitoring processes. This process is based upon the risk management process developed by the Department of Defense in 1996-1997 and first published in 1998. While the process steps differ from the 1996 PMI® *PMBOK® Guide* (e.g., risk planning and monitoring process steps are added), they are consistent with the risk management process that may appear in the next edition of the *PMBOK® Guide* (risk management planning, risk identification, risk assessment, risk quantification, risk response planning, and risk monitoring and control).

NASA imposed minimal contractual requirements for risk management on Hyperion, limited simply to “develop a comprehensive, proactive Risk Management Plan.” Yet, because of the GIS and WIS project terminations, there was *substantial* NASA interest in developing, implementing, and continuously performing effective risk management on Hyperion far beyond the apparent importance of a single sentence.

Risk Planning

Risk planning is the process of developing and documenting an organized, comprehensive, and interactive strategy and methods for: (1) identifying and tracking risk issues, (2) developing and implementing risk handling plans, (3) monitoring risks to determine how they have changed, and (4) documenting the overall risk management process.

Inputs to risk planning included the Hyperion budget, NASA performance requirements, and the project schedule.

The primary output of risk planning was the Hyperion risk management plan (RMP), which included: (1) a description of the risk management process steps, (2) organizational responsibilities, (3) discussion of likely risk categories, (4) risk identification methods, (5) a detailed risk analysis methodology, (6) a risk ranking procedure, (7) guidelines for developing risk handling strategies, (8) risk monitoring techniques, and (9) suitable reporting forms to be applied to candidate risk issues for each process step.

The first risk management activity performed on Hyperion was to tailor an RMP to the project based on RMPs developed for large-scale projects (e.g., multibillion-dollar life cycle cost). This was done to ensure that the resulting process and implementation strategy would work on a program (Hyperion) where a single week was viewed as a long period of time. Here, each implementation step and activity was carefully weighed to determine if it brought value added, yet would not impose a burden on available resources. For example, a set of ground rules and assumptions were developed that described the project, including key technical characteristics and schedule milestones. These later proved important for accurately identifying and analyzing project risk issues.

After the RMP was developed, risk management training was given to most project engineers and managers. Following this training, the project manager, deputy project manager, and the risk management consultant identified a key risk issue, performed an initial risk analysis, and developed a risk handling plan (RHP, also known as risk response plan) for that issue. The results were documented, presented to and critiqued by the project team.

This “trial case” provided insight to the entire team how risk identification, analysis, and handling would be performed. It also demonstrated that Hyperion upper management was personally involved with risk management, and supported its implementation. The value of this and subsequent actions performed by Hyperion management cannot be understated. Without upper management support and participation the effectiveness of the risk management process would have suffered, and may lead to substantial problems on this relatively high-risk project.

A risk management board (RMB) was established and included key project personnel. While the RMB met monthly, progress meetings were held daily and included all RMB personnel. The project manager and deputy project manager encouraged discussion of risk-related issues during these meetings. When new issues were identified or an unfavorable trend in re-

solving an existing risk issue appeared, specific guidance was provided to address the concern. Hence, while the RMB met monthly, its constituents *met daily* and immediately addressed risk-related questions as they appeared.

Finally, the Hyperion RMP was routinely used during the course of the project program rather than being a document that gathered dust—it was *the* risk management reference guide both for describing the process and how it was implemented.

Risk Identification

Risk identification is the process of examining the program areas and each critical technical process to identify and document the associated risk.

Inputs to risk identification included: (1) the project WBS, (2) the project budget, (3) the project schedule, (4) data collected from other projects (e.g., capabilities associated with analogous hardware and software developed for the previous projects), (5) NASA specified performance requirements, (6) information about key processes, and (7) the RMP.

Tools and techniques used for risk identification primarily included: (1) evaluating lessons learned from analogous projects, (2) brainstorming and interviewing key project personnel, and (3) risk review questions that served as indicators of potential risk issues.

In performing risk identification we evaluated candidate risk issues in accordance with the program’s WBS, together with risk categories defined in the RMP for hardware, software, and integration items. Hence, the risk identification step followed a repeatable, structured process, which is superior to what is done on many programs where a WBS is not used, nor are likely risk categories defined for different program items.

When performing the initial and subsequent risk identification activities, we were careful to consider not only risk issues associated with the item in question, but also potential inter-relationships with other items as well. For example, for two different electronics assemblies there were no identified resource risks when the assemblies were considered separately. But when resources were considered for both assemblies, the availability of qualified assembly personnel was identified as a risk issue. Had the interrelationship between assemblies not been examined, this risk issue would not have been identified until it later became a problem, with potentially nontrivial cost and schedule impact to the project.

The outputs from risk identification included a list of risk issues, a detailed description of their cause, likely risk probability categories (e.g., hardware technology maturity), and the likely impact (consequence of occurrence) categories (e.g., cost). The documented risk issues then became an important input to the risk analysis step.

Risk Analysis

Risk analysis is the process of examining each identified risk issue or process to refine the description of the risk, isolate the cause, and determining the level of risk present.

Inputs to risk analysis included: (1) identified risk issues, (2) uncertainty associated with the project schedule for key activities, (3) ordinal probability and impact scales, and (4) the RMP.

Tools and techniques used for risk analysis included: (1) interviewing key project personnel (e.g., expert judgment), (2) ordinal probability and impact scales, (3) a risk mapping matrix, and (4) Monte Carlo simulations (for schedule risk analysis).

The primary tool used for risk analysis was ordinal probability and impact scales. Here, previously developed scales were tailored specifically to hardware, software, and integration risk issues. For example, for hardware risk issues, six probability scales were used. For software and integration risk issues, four and two probability scales were used, respectively. In addition, each software risk issue was also evaluated with the integration scales to capture potential hardware/software and other integration risk concerns. Three impact scales were used for evaluating each risk issue (cost, performance, and schedule (C, P, S)).

The probability and impact scores were converted to risk level (low, low medium, medium, medium high or high) using a risk mapping matrix. We developed separate risk levels for each item based upon the maximum of the combination of the probability and impact scores for C, P, S. Thus, three risk scores associated with C, P, S were reported for each risk category. For example, for a hardware-related risk issue we reviewed the 6x3 (18) total probability and impact pairs and took the maximum of the six probability and impact pairs for cost, performance, and schedule (thus yielding three risk scores). (Had we chosen to do so, we could have reduced the three risk levels for each risk issue to a single score by taking the maximum of the risk levels determined for C, P, S impact.) Risk issues with a cost, performance, or schedule risk level of low medium or higher were then tagged to develop an RHP. While on some programs a risk level of medium or higher would be suitable, because of the stringent Hyperion schedule, low medium risk level was used.

We also performed a Monte Carlo simulation against the project assembly and test schedule to identify the probability of achieving key project milestones, including the delivery date. (This was of considerable consequence since there was roughly a \$50,000 per day penalty for late delivery and a \$50,000 award per day for early delivery against the contractually specified delivery date.) The assembly and test schedule module was extracted from the program's master schedule and evaluated using a Monte Carlo simulation add-in to the project scheduling software. Key activities were identified that, based upon past experience, were likely to contain schedule estimating uncertainty and/or technical risk. We modeled these two items by use of a single distribution. Interviews were used to estimate the resulting probability distribution critical values. We used cumulative, general, histogram, and triangle distributions to represent the probability distributions based upon inputs from the experts being interviewed. The simulation was updated approximately three times a month and the project manager used the simulation outputs for planning purposes and reporting to senior management.

Outputs from risk analysis included: (1) prioritized risk levels for risk issues, (2) a watch list for low risk issues, (3) confidence levels for achieving key project schedule milestones (e.g., what probabilistic percentile did the critical path method delivery date correspond to), and (4) durations and finish dates associated with key portions of the assembly and test schedule.

Risk Handling

Risk handling is the process that identifies, evaluates, selects, and implements strategies in order to reduce risk to an acceptable level given program constraints and objectives. This includes the specifics on what should be done, when it should be accomplished, who is responsible, and associated cost and schedule.

Inputs to risk handling included: (1) prioritized risk levels for risk issues (with risk levels low medium or higher), and (2) the RMP.

Tools and techniques used for risk handling included: (1) assumption, (2) avoidance, (3) control (mitigation), and (4) transfer.

Often times, control is the default option selected; yet it may not be the best risk handling option. For all risks analyzed as low medium or higher, the four handling options were evaluated in terms of feasibility, expected effectiveness, cost and schedule implications, and the effect on the system's technical performance, and the best option selected. A suitable approach for implementing the risk handling option was also developed. This led to the primary risk handling strategy. In cases where the risk was evaluated to be medium high or high, one or more backup strategies were also developed.

For example, for one optical component a backup strategy involving parallel development with a second vendor was implemented. (Here both the primary and secondary strategy used the control option.) When the optical elements from both vendors were tested, the backup unit passed the performance tests and was selected, while the primary unit would have introduced a substantial performance degradation and was rejected. Had the backup strategy not been pursued, the project would have been suffered a substantial adverse cost and schedule impact, and could possibly have possibly been canceled. In another case a change in the launch vibration load imposed on Hyperion led to the development of a primary risk handling strategy and two backup strategies because of the potential for major project impact. Here, the primary strategy failed a proof load test and the initial backup strategy was rejected due to minimal performance margins. However, the second backup strategy passed its qualification test and was accepted. Had the second backup strategy not been exercised, the project would also have been suffered a substantial adverse cost and schedule impact, and could possibly have been canceled.

Outputs from risk handling included: (1) an RHP for each selected risk issue with a variety of information about the primary (and any backup) option and approach selected, activities needed to implement the strategy, key schedule milestones, the anticipated residual risk level, estimates of funding, schedule, and

other resources needed (e.g., test equipment); (2) integration of RHP information with the project schedule; (3) the need for contractual mechanisms with additional vendors and suppliers to perform risk handling activities; and (4) inputs to other processes (e.g., reallocation of funding between project activities and obtaining assurances that suitable personnel and resources will be available as needed).

Risk Monitoring

Risk monitoring is the process that systematically tracks and evaluates the performance of risk handling actions. Essentially, it compares predicted results of planned actions with the results actually achieved to determine status and the need for any change in risk handling actions.

Inputs to risk monitoring included: (1) the RHP for each approved risk issue and (2) the RMP.

Tools and techniques used for risk monitoring included: (1) earned value (cost variance), (2) variations against the project schedule, and (3) the use of technical metrics in some cases.

In Hyperion, the use of daily progress meetings provided key personnel the opportunity to explore in real-time the C, P, S progress of implementing risk handling strategies. This was very important given the high degree of schedule compression that existed on the project (about 4:1).

The key risk monitoring metric used was variations against the project schedule because of the very short development and integration time available (about six months each), coupled with the roughly \$50,000 per day penalty for late delivery and \$50,000 award per day for early delivery against the contractually specified delivery date. Project schedule updates were performed weekly and attention was given to prioritizing resources, and re-ordering tasks and performing others in parallel where appropriate in order to maintain or even shorten the schedule without increasing the level of schedule risk.

Outputs from risk monitoring included: (1) inputs to risk handling (update RHPs as needed), (2) inputs to risk analysis (information that may represent changes in probability and impact scores), (3) inputs to risk identification (information that may represent new risk issues or changes to existing risk issues), and (4) inputs to the monthly risk management report.

Discussion

While some lessons learned from Hyperion are unique to that program, the following are some key findings that can likely be transferred to many other types of projects.

General Observations

The Hyperion experience demonstrated that proactive risk management can be implemented and highly effective on even short duration, relatively small budget projects. For example, if a suitable risk management process and expert risk management consultation is available, there should be little or no reason for

avoiding performing comprehensive risk assessments. In fact, on Hyperion we performed six comprehensive risk evaluations (one initial evaluation plus five updates) and documented the findings *in a seven-month period of time*. This is far more “intensive” than what exists on virtually any project, including those with substantially greater budgets and longer development schedules, yet the almost monthly updates were performed using only about two man weeks of labor. (Of course, had the risk management consultant had less experience the amount of resources needed to perform the risk evaluations would have been substantially larger.) Perhaps just as importantly, the comprehensive nature of the monthly risk evaluations helped persuade NASA upper management to continue funding Hyperion because they could see the progress being made to reduce risk issues to an acceptable level both in a clear and timely manner. (NASA management stated on more than one occasion that the quality of risk management performed on Hyperion greatly contributed to the success of the project and kept it from being terminated.)

The risk management process should be comprehensive (e.g., include all risk management steps), but tailored to the project and eliminate nonessential activities. Attempting to copy a risk management process or its documentation from one project to another and blindly apply it will greatly diminish its effectiveness, if not lead to failure—expert tailoring and implementation are needed.

Key management involvement is *absolutely essential* for effective risk management. However, it is unfortunately commonplace for project managers to either not embrace risk management, or not actively participate in risk management activities, or not appoint a risk management proponent with sufficient knowledge, authority and clear direction to effectively implement the process. Often working level engineers interpret these behaviors as representing a lack of upper management interest. This can have a severe negative impact on the overall risk management effectiveness, and can adversely affect the overall level of project success. The success of Hyperion was well correlated with the desire and active participation of the project manager and deputy project manager to effectively perform risk management. This provided a key leadership example to project engineers rather than just lip service.

Project managers should encourage “out of the box” thinking so long as necessary technical procedures (e.g., related to quality) are not violated. In one case where epoxy had to be removed from a cryogenic cooler component, the cognizant manager brought in a local dentist who successfully drilled-out the fixture. He correctly reasoned that dentists had a high skill level in performing this type of drilling—much more so than engineers who had never before attempted it.

The savings from a single successfully averted risk issue paid for the *entire risk management program many times over*. The use of parallel development for a single optical component (discussed in Section 3.5) led to a 120:1 return on investment (based upon constant year dollars) when the primary vendor failed to

produce an acceptable part. Here, an investment of \$15,000 averted a project charge of about \$1.8 million (because the component was on the project's critical path). And in this case, the savings from this one item was greater than the cost of all risk management activities added to the original development plan!

A monthly risk evaluation report was prepared and delivered to NASA that provided a comprehensive view of all identified project risks, the analyzed risk levels, and status of RHPs. The initial risk management report served as the template for subsequent reports, so the amount of resources needed to update it monthly was not substantial (about 1.5 man weeks after the first report).

Last and most importantly, a suitable attitude toward risk management is necessary for its success. A culture shift occurred which included risk management as part of the daily decision making process. Project managers and engineers became committed as evidence of risk management "successes" repeatedly solved risk issues and averted problems. This is extremely important, since a "check the box" approach to risk management will almost never be effective.

Some Observations Related to the Risk Management Process Steps

Some formal risk planning is desirable prior to performing the initial risk assessment. This will help to identify likely risk categories, necessary ground rules and assumptions, etc. The initial risk planning performed (discussed in Section 3.1) was a key contributor to the overall risk management success. For example, had this planning not been performed it is likely that one or more key risk categories would not have been included and the ground rules and assumptions needed for risk assessment would have been incomplete or flawed.

Risk identification should be fairly comprehensive to minimize the number of risk issues going undetected. We used the project WBS and evaluated key processes in order to accomplish this.

The use of a structured, carefully constructed risk analysis approach (in this case ordinal scales) increased the accuracy and repeatability of results versus had purely subjective estimates been used. In addition, the approach we used greatly simplified performing risk analysis updates because the technical experts were able to examine the preceding risk analysis, note changes in the item's maturity, and quickly estimate the "probability" and consequence of occurrence levels that existed at that time.

The development of brief, written RHPs helped identify implementation steps that otherwise would have been missed. For example, on several occasions risk issue focal points noted that the structured approach used to develop the RHP steps and associated milestones led them to include additional steps that were needed to properly implement the risk handling strategy. The development of RHPs also helped identify when backup risk handling strategies were desirable.

The use of one or more backup risk handling strategies may be warranted, if not essential, for some risk issues. As discussed

in Section 3.5, in two different cases there was no reason to initially doubt the feasibility of the primary risk handling strategy, yet in both cases it failed. In each case, a viable backup risk handling strategy not only was successful, it may well have prevented the cancellation of the program because of the potential for substantial schedule slippage.

Risk monitoring metrics should be carefully tailored to the program. For example, on Hyperion relatively few technical performance measurements (TPMs) were used for formal tracking and subsequently reporting risk handling implementation because the duration associated with many project activities was quite short. Instead, test results were sometimes reported and discussed at the daily engineering management meetings and changes in the risk handling strategy were occasionally made as needed. (Again, personnel attending these daily meetings also constituted the RMB, and had the knowledge and authority to recommend such changes.) However, on development or production projects that do not have substantial schedule compression, TPMs often prove valuable for monitoring progress in implementing the risk handling strategies.

References

Department of Defense. (1998, March). *Risk Management Guide for DoD Acquisition*. Defense Acquisition University and Defense Systems Management College, First Edition, Ft. Belvoir, VA. (Substantial enhancements were included in the second edition of this document, published in May 1999. The current version is the third edition, published in January 2000.)