**SOFTWARE PROCESS ENGINEERING PROJECT**

***Contributed by Dan Shoemaker, Professor, Center for Cyber Security and Intelligence Studies, University of Detroit Mercy***

**Operating Scenario: Heavy Metal Technology**

Heavy Metal Technology (HMT) is a general technology holding company whose line of business is tailored to the provision of advanced weapons systems to the United States Army. Heavy Metal Technology’s various subsidiary companies are maintained as one coordinated business entity from offices in Sunnyvale, California. The centralization of policy and planning direction at one location has historically produced high revenues, profit margins, and customer satisfaction. The necessary degree of coordination is enabled by a global, enterprise network that is managed from the Sunnyvale location.

Heavy Metal’s holdings are concentrated in advanced technology products and services to the military. Two closely held subsidiaries deal exclusively with the Federal government. The line of business of one, which is based in Gaithersburg, Maryland, is component research and development (R&D) and manufacture for advanced capability pods for the AH-64D Apache Longbow helicopter. The other, based in Jacksonville, deals in advanced electronics integration for the Army. There is also a manufacturing facility in Detroit. That facility builds Leopard tanks for the Canadian Army under license from the German government.

Other close holdings in Heavy Metal’s empire include a commercial electronics R&D facility in Corvallis. The Corvallis facility also does contract work for the Idaho National Laboratory. In addition to the closely held corporations, there are loosely held electronics manufacturing holdings in Pittsburgh, Houston, Des Moines, Sioux Falls, Denver, and Bozeman. All of these serve the commercial electronics industry.

Finally, there are a number of loosely held international corporations in India, Australia, and across the Pacific Rim, all concentrated on software code development. All computer services for that region are provided over a public/private VPN (Virtual Private Network), which is maintained for that area in Singapore. The Singapore data center is actually owned and operated by Heavy Metal, as part of the company’s global VPN. The VPN itself is maintained out of the Sunnyvale office.

According to Heavy Metal’s charter, the primary goal of the business is to “target the best business opportunities, win new business, and to deliver increased customer satisfaction.” Heavy Metal Technology entered the market knowing that the ability to deliver high-quality products to its customers would be a prerequisite to its success. In fact, its entire business model was based on the presumed ability to do that. Because it was the key to company survival, that mission was laid out even before the technical capability for achieving it was in place.

Heavy Metal Technology’s information processing operation delivers information and services to its various subsidiaries in two ways: hosted and embedded. The hosted model removes the burden of maintaining on-site data acquisition and management functions from the facility’s operations managers, while ensuring a secure and scalable worldwide environment. The embedded model allows each local facility to operate and maintain its own Information Technology (IT) infrastructure, which is tailored around Heavy Metal’s enterprise systems to support that subsidiary’s specific line of business and business operation.

**Business Case: IT Operation**

Heavy Metal Technologies is a relatively small corporation by Pentagon standards (approximately $350 million a year) but it has an exceptionally good record of achievement in the area of upgrading operational electronic combat systems to new, or improved equipment standards. As such, it enjoys an extremely strong, long-standing relationship with virtually all branches of the Department of Defense (“DoD”), as well as several defense prime contractors. It has a very large installed base of products, a number of sole source contracts, and a strong management and advisory team.

Heavy Metal Technology targets component integration. Because parts of these products must be developed, the company relies on the RFP (Request for Proposal) process up and down its supply chain. The business itself involves custom development and so the actual development process typically must accommodate large numbers of engineering change orders during the course of the process. The company’s current focus is on designing and building custom electronics, but other business verticals will be targeted in the future, especially healthcare electronics and data services

Heavy Metal Technology knew that it could not have its subsidiaries on separate governance systems since that complexity would prevent it from controlling its various holdings. Separate governance systems would also far outstrip the ability of the company to cope with the problems raised by evolving business ventures in each subsidiary. So it brought the relevant aspects of the governance of all of its ventures under the umbrella of a single system.

**Environmental Considerations**

Heavy Metal Technology wants to monitor the interface with the business process through quantitative data. The primary reason for that is that Heavy Metal wants good data to base “hold-or-fold” business decisions on. The problem is that the complexity of tracking an unknown number of business transactions across a large variation of industries would completely overwhelm the company’s relatively small central staff without considerable IT support. Nonetheless, the problems that complexity and volume represent also cause considerable wear and tear on the management staff.

Therefore, Heavy Metal wants to put strong process safeguards in place. Strategic security concerns, such as keeping all of the software engineering functions in the organization aligned with organizational goals, dealing with changing events in the tech environment, making sure that the right people are involved in the decision making process, keeping the architecture of the software engineering processes simple, and establishing a reliable response to market conditions, are all considerations.

In particular, maintaining alignment between its software integration processes and the company’s overall vision is a central theme for Heavy Metal Technology executive managers. And the idea of coordination and communication as a way of thinking permeates the business operation. The fundamental commitment to keep everyone in the business and its holdings on the same page in terms of deciding where the company is, and is not, going to invest is a central theme of upper management. This capacity for working synchronously toward a common goal through strong communication and process discipline is the essence of the Heavy Metal Technology business model.

**Business Architecture**

Every successful company depends on the right business architecture. For Heavy Metal Technology, this meant an architecture that blended general concerns that decision makers have data available to support informed decisions.

Heavy Metal Technology uses COTS software when possible, but it does not hesitate to build its own components when necessary or to mitigate risk. Heavy Metal Technology’s major concern about COTS products centers on its ability to ensure its security. That was particularly true when targeted bench-checks found inherent defects embedded in products that were acquired from an overseas source. Thus, supply chain security is essential.

Where the source of the code is in doubt, Heavy Metal Technology will not hesitate to build the necessary components in-house. The Heavy Metal Technology rule of thumb is that if the function is unimportant, COTS will do. If there’s an actual or de facto security requirement for some aspect of the system, the COTS product will have to be proven secure. Otherwise, that component is a strong candidate for in-house implementation.

**Data Collection, Metrics, and Tracking**

Heavy Metal Technology uses metrics as a key planning tool. For each critical software item in its inventory, Heavy Metal Technology measures the:

1. Projected number of threats with impact (as likelihood percent)
2. New threats identified (as frequency)
3. Actual number of incidents (as count)
4. Time/date of the incident
5. Cost of the incident
6. Violations involving staff (as incident count)
7. Number of software defects reported (as count)
8. Number of software defects repaired (as percent)
9. Cost of repair

**Structuring the Organization**

In order to maintain up-to-date planning, documentation, and oversight of organization-wide security policies and procedures, Heavy Metal has formalized an executive management team and various ad-hoc task teams, who report to the Chief Executive Officer of the company. In some instances, for specific technology decisions, the teams report to the Chief Information Officer.

Heavy Metal Technology has allocated a small percentage of its support staff resources to administrative coordination of the work of the teams. The teams constitute an “elite” group of Heavy Metal Technology worldwide group of software engineers. Although the personnel on the teams represent a low percentage of the total number of software engineering staff, they are influential when it comes to formulating the shape of the overall product architecture. This scheme instantiates Heavy Metal’s strategic governance-oriented lifecycle and affects the work of all of Heavy Metal Technology development personnel. The corporate CISO (Chief Information Security Officer) is responsible for providing quarterly status reports on the state of the governance system and any emerging concerns. This artifact is considered a matter that requires board-level attention and therefore it has a formal standing in the annual report. The report itself is written at a non-technical level in order to promote understanding across the company.

**Detail of the IT Operating Model**

Early software project planning is stressed at HMT, and project plans are developed to integrate effectively with the other engineering plans within each project. There is strong informal communication among all the engineering disciplines, and a single program manager manages each new project from an integrated system view. Software estimates are derived through expert analysis and documented for use throughout the project's life. These estimates are backed up with outputs from estimation tools that are used to provide a ”reality check” to the experts’ initial idea. Actual project data is retained to support an estimation improvement effort underway at HMT, but it is not used in a formal feedback sense.

Software project management metrics are used to provide visibility into project performance at the project level. When performance deviates from the initial plans, the project manager is responsible for either making changes to the way the project is being handled (in order to bring the project back into conformance with the plan) or re-planning. Software subcontracts are managed using a set of defined policies and procedures.

Software requirements, design, and code inspections are used to support development. Defect metrics from the inspections are maintained. Other product-related metrics are identified and maintained for each development effort to help keep reasonable visibility into the development effort. These metrics also are used to support software project management and risk assessment. The only problem is that all of this takes place at the project rather than the organizational level. The program manager and upper management never see the results of this extensive measurement process.

The review culture at HMT is not well developed. The reason for that is because SQA (Software Quality Assurance) is primarily defined as testing and there is no formal change management process. A SEPG (Software Engineering Process Group) team of engineers and managers from the software engineering organization are responsible for keeping the approved software engineering processes up to date, and identifying new opportunities for improvement. This team reports to the manager of software engineering and to the corporate vice president of engineering. The vice president of engineering maintains a keen interest in the software engineering processes for the corporation. The manager of software engineering and the vice president of engineering are responsible for providing quarterly reports to the company president on the state of software engineering and software process improvement. The problem is that most of this is rumor rather than fact based.

There have been extensive testing, reviews, audits, verification, and validation activities performed on mission-critical systems by the programming staff. The manager of each functional area is responsible for contracts. They are also responsible for general supervision. On the traditional IT side of the operation, Heavy Metal employs three managers: one for Development (13 analysts and 55 programmers), one for Maintenance (10 analysts and 33 programmers) and one for Operations (187 systems staff and 48 programmers). There are no supporting or quality management services. IS (Information Systems) security is conducted as a separate function from the network and IT function.

Finally, in the largest sense, there are at least five communities of practice involved with Heavy Metal Projects: Acquirers (both internal and external), Suppliers (both internal and external), Developers (both internal and external), Operators (both internal and external), and Maintainers (both internal and customer). There is also a large and sophisticated network operation that is conducted separate from the IT function.

**The Specific Case**

Heavy Metal’s Electronic Combat Systems Group (ECSG) is located in three places in North America, specifically in Gaithersburg, Maryland (which specializes in the design and production of electronic warfare [EW] systems) and Corvallis, Oregon (which provides circuit card assembly, electromechanical assembly, and environmental testing). However, the main production operation is in Jacksonville, Florida, which actually constitutes four facilities.

HMT was contracted by the Army to upgrade the target acquisition and display fire control system for the AH64-D Apache Longbow attack helicopter. This is a field upgrade of the current analog system used by the Apache; thus, it is considered a modification of an off-the-shelf (COTS) product. However, even though the work is done on a legacy system, modifications to the code will be necessary in order to integrate a GPS (Global Positioning System) and enhanced communication capability into the aircraft. Revisions of the current system will need to be written (and/ or modified) to support the following functional requirements:

1. Integrate the GPS into the existing navigation system.
2. Display updated navigation information on the pilot's Head-Up Display (HUD).
3. Allow the pilot to be able to input and modify navigation and fire control data through an onboard Control Display Unit (CDU).
4. Communicate GPS and targeting information to ground control and to other aircraft on the mission. (Note: no equipment upgrades are planned to support the increased communications requirements.)

In the case of the GPS/CDU upgrade, the product will be a working GPS interface with the CDU. This project can also be viewed in terms of its constituent management processes. In this case, the major processes are project management, software development support, software development, software qualification, and post-development support.

The requirements of the GPS Interface are well known. The software in the current onboard navigation system and interface software is written in C++, and due to the nature of the changes required for the navigation components, no change in the language platform is being considered. The contractor who will supply the GPS system will make modifications to the GPS software that will allow it to be interfaced directly to the overall system. This will be done on a subcontract to HMT. HMT will provide a specification of the modification requirements to the subcontractor. This will reduce the cost and risk associated with that aspect of the overall system development process.

HMT has determined that about 9,000 SLOC overall will have to be developed and/or modified in order to integrate the GPS into the current fire control system. Because configuration management has not been practiced in the past maintenance of the system, the existing navigation software has not been fully validated and the customer wants formal documentation. Therefore, it was assumed in the initial planning that the development process itself would most closely resemble that for a new project.

The Army (acquirer) has contracted to supply a valid System/Subsystem Specification (SSS), a System Design Description (SSD), and an Operational Concept Document (OCD). The Army will modify the OCD during development to reflect any requirements or changes that might emerge as the process progresses downstream. HMT will be responsible for the following technical documents:

1. Software and Interface Requirements Specifications (SRS & IRS)
2. Software and Interface Design Descriptions (SDD & IDD)
3. Software Test Plan (STP)
4. Software Test Description (STD)
5. Software Test Report (STR)

HMT will also be responsible for the following management and support documentation:

1. Software Development Plan
2. Software Transition Plan (STP)
3. A Software Version Description (SVD)

**Project Requirements**

Based on preliminary project planning, it is estimated that the software effort will take approximately 3.25 person-years over a period of 12 months. The development, test, and technical documentation effort will be approximately 2.25 person-years; the remaining 1.0 person-year will be dedicated to software project management, managing the support documentation, SQA, and SCM (Software Configuration Management). User documentation will be produced as part of the new CDU development effort. The GPS subcontractor will develop the SRS and SDD for the GPS from existing materials created for the general product.

The pilots for this aircraft dislike the old CDU and want a replacement. The current CDU has a very small keypad, and the display is only four lines by 40 characters. The pilots would like to at least double the display capacity, increase the display visibility, change the keypad, and add new query capabilities. The pilots want an opportunity to help determine the requirements for the CDU and to have significant inputs to user interface changes.

Because the pilots want so much involvement, the Army is pushing to have individual field personnel, who they will authorize, involved in the actual development process. Since that is the case, HMT feels that prototyping will be useful to support user interface development. In addition, it is not known how many new capabilities will be added to implement the pilots' query requirements. HMT is assuming that the new CDU will have all new software. The Army wants the new CDU to be implemented in Java, and the existing code is in assembly language, so it is assumed that there will be no software code reuse. Furthermore, the Army is requesting significant amounts of formal documentation.

Based on HMT's knowledge of the existing CDU and a rational appraisal of the possible new requirements, HMT assumes that the new CDU will require about 20,000 SLOC to implement. Given the unknown nature of the new requirements, this is a soft estimate. The customer wants the new CDU to be a significant improvement from the current version, so there may be some flexibility to re-negotiate the terms of the contract when the first sets of prototypes are completed and approved by the pilots. In both parts of this upgrade project, software supportability is a primary concern. Thus, planning for the software transition to the Government and for Post Deployment Software Support (PDSS) is stressed in the acquisition. This may add labor to the existing software estimates from HMT.

**Summary: Project Characteristics**

Here is some additional information that you might need:

* The project size is approximately 29,000 total SLOC.
* There are five interfaces involved between the user, the GPS, and the CDU.
* There are 150 aircraft in the inventory to be upgraded. There will be one user for each aircraft. It is assumed that the aircraft will remain in service for at least another decade.
* There are approximately 800 pages of documentation.
* There will be a subcontract for modifications to GPS code and for new (or modified) GPS documentation.
* There is minimal technical complexity.
* It is classed a life-critical application.
* There is a moderate need for management visibility.
* Because it is life critical, assurance needs to be employed sufficient to assure that the aircraft requirements have been reliability met.

The areas for concern are security, human safety, the level and degree of formal software engineering methods that will have to be employed, the need for formal reviews and signoffs among a number of dispersed entities, and the relationships with subcontractors. On examining the project characteristics, the project manager notes the following regarding these issues:

* Adding the GPS to an existing aircraft is a known problem and the system will be small; thus, a waterfall lifecycle can be used. [Please note that this is a single system component that will be integrated into the larger solution at a later date. Whatever lifecycle approach is employed by HMT for the larger solution needs to consider and accommodate the approach that is employed for this component.]
* Reliability will be stressed during testing. This is already documented in the corporate handbook on metrics for life-critical or safety-critical systems.
* There is a need for in-process reviews for this project.
* Since the security assurance process is new to the organization, it will be important to track progress and results for this project.
* The metrics practices are internal; they do not cover sharing data with the acquiring organization (e.g., the Army).
* Although risk management practices will be used, nothing in the approach to risk management has been defined for this application.
* The project manager is responsible for maintaining all compliances and for developing the risk and continuity management plans.

**Your Assignment**

Because the contracted enhancement is so important to the continuing success of the main ground attack helicopter program and because of its importance to national defense, the Army wants a total commitment from HMT that the integrity of the project information will be assured. In order to do that, HMT must organize this project into a well-defined architecture of logical and reliable processes. Therefore, you will do two large projects for this exercise.

**First [Lifecycle]** - Select and justify a lifecycle model that is both appropriate to the business environment of the case as well as the project requirements of the AH64D Longbow project. Explain why the model was selected (e.g., What advantage does it give and what are you trying to foster/prevent by adopting it?). Provide a point-for-point explanation of why you chose a particular approach.

**Second [Maturity Model]**– select and justify an appropriate organizational/project security capability process improvement model, which both fits the business environment of the case as well as the project criticality requirements. Likewise, explain why the model was selected (e.g., What advantage does it give and what are you trying to foster/prevent by adopting it?). By way of explanation, make a suggestion as to how HMT can restructure its operating environment to achieve the level of process capability maturity necessary to assure that the project code is both qualitatively correct and secure.