Applied Space Systems Engineering
Chapter 17 Manage Technical Data
28 May 2008

Effective space systems engineering (SSE) is conducted in a fully electronic manner. Competitive hardware, software, and system designs are created in a totally digital environment that enables rapid product design and manufacturing cycles, as well as a multitude of techniques such as modeling, simulation, and lean manufacturing that significantly reduce the lifecycle cost of systems. Because the SSE lifecycle depends on the digital environment, managing the enormous volumes of technical data needed to describe, build, deploy, and operate systems is a critical factor in the success of a project.

This chapter presents the key aspects of Technical Data Management (TDM) within the SSE process. It is written from the perspective of the System Engineer tasked with establishing the TDM process and infrastructure for a major project. Additional perspectives are reflected from the point of view of the engineers on the project who work within the digital engineering environment established by the TDM toolset and infrastructure, and from the point of view of the contactors who interface via the TDM infrastructure. Table 17.1 lists the TDM process as it relates to SSE.

Table 17.1 Applied Space Systems Engineering Technical Data Management Process.

Step	Description	Chapter 17 Section	Detail Chapters
1	Prepare a Strategy for the Conduct of Technical Data Management	17.1	X
	Identify engineering lifecycle requirements for technical data	17.1.1	X
	Determine required data content and form and electronic data exchange interfaces in accordance with international standards or agreements	17.1.2	X
	Establish a framework for technical data flow within the project technical processes and to or from contractors	17.1.3	X
	Designate technical data management responsibilities and authorities regarding origination, generation, capture, archiving, security, privacy, and disposal of technical data work products	17.1.4	X
	Establish the rights, obligations and commitments regarding the retention of, transmission of, and access to technical data items	17.1.5	X
	Establish the strategy for relevant data storage, transformation, transmission, and presentation standards and conventions to be used in project or program policy, agreements, and legislative constraints	17.1.6	X
	Describe the strategy for the methods, tools, and metrics used during the technical effort and for technical data management	17.1.7	X
	Prepare the training strategy for appropriate technical team members and support and management personnel in the established technical data management strategy and related procedures and tools	17.1.8	X
2	Collect and Store Required Technical Data Artifacts during the Engineering Lifecycle	17.2	X
	Identify existing sources of technical data artifacts that are designated as	17.2.1	X

	outputs of the common technical processes		
	Collect and store technical data in accordance with the technical data management strategy and procedures	17.2.2	X
	Record and distribute lessons learned	17.2.3	X
	Perform technical data integrity checks on collected data to confirm compliance with content and format requirements and identifying errors in specifying or recording data	17.2.4	X
	Prioritize review, and update technical data collection and storage procedures	17.2.5	X
3	Maintain Stored Technical Data	17.3	X
	Review and release system engineering artifacts	17.3.1	X
	Update and revise system engineering artifacts	17.3.2	X
	Manage the databases to maintain proper quality and integrity of the collected and stored technical data and to confirm that the technical data is secure and is available to those with authority to have access	17.3.3	X
	Perform technical data maintenance as required	17.3.4	X
	Prevent the stored data from being used or accessed inappropriately	17.3.5	X
	Maintain the stored technical data in a manner that protects it against foreseeable hazards such as fire, flood, earthquake, and riots	17.3.6	X
	Backup and archive artifacts for recovery and future uses	17.3.7	X
4	Provide Technical Data to Authorized Parties	17.4	X
	Maintain an information library or reference index to provide data available and access instructions	17.4.1	X
	Receive and evaluate requests for technical data and delivery instructions	17.4.2	X
	Confirm that required and requested technical data is appropriately distributed to satisfy the needs of the requesting party and in accordance with established procedures, directives, and agreements	17.4.3	X
	Confirm that electronic access rules are followed before allowing access to the database and before any data is electronically released or transferred to the requester	17.4.4	X
	Provide proof of correctness, reliability, and security of technical data provided to internal and external recipients	17.4.5	X
5	Collaborate through Effective Use of System and Process Artifacts	17.5	X
	Use collaboration tools and techniques	17.5.1	X
	Use search and retrieval tools and techniques	17.5.2	X

At the highest level, digital information is created, managed, and used in two broad forms: 1) as structured data resident in database management systems (or other systems that provide standard access and retrieval capabilities) and 2) as digital content (simply referred to as content from this point on, residing in repositories of various forms.

Structured data is created, stored, and managed in a precisely defined fashion—typically in the relational database form consisting of tables constructed of logically defined rows and columns storing instances of data. Structured data is created as part of well-defined transactions via interfaces (often user interfaces) that are developed for entering, updating, and using structured data. Manufacturing orders and financial transactions are classic examples where digital information is generated and stored as structured data.

Content, on the other hand, is digital information that takes on many forms as its created by the author of the data. Documents, digital images (still and video), spreadsheets, business presentations, email, web pages, and web blogs are just some examples of digital content that span a vast range of formats depending on the objectives and needs of the author.

An artifact in a digital engineering environment is data or content created during the SSE lifecycle that relates to the system being developed or to the lifecycle itself. Artifacts range from System Requirements Specifications, Computer Aided Design (CAD) drawings and specifications, Engineering Bills of Materials (EBOMs), and Interactive Electronic Technical Manuals (IETMs), to design review comments and findings, to metrics on the labor hours required to complete the requirements phase of the lifecycle. In the digital engineering environment, electronic artifacts are the means by which systems are defined, specified, reviewed, and in certain cases, delivered. Effective systems to create, manage, and use electronic artifacts are essential to rapid and cost effective delivery of the Space Systems they support.

Editors Note: The Figures and Tables in this chapter are based on Engineering Policies and Procedures of United Space Alliance, LLC. Used with permission.

17.1 Prepare a Strategy for the Conduct of Technical Data Management

A successfully strategy for the conduct of TDM is closely aligned with an organization's goals and objectives for system engineering. A System Engineer tasked with establishing the TDM process and infrastructure for a major project explicitly seeks out these goals and objectives in order to align his or her strategy accordingly. A key factor for success in this arena is an understanding of SSE processes and their relationships to one another. This in turn allows each process or sub process to be optimized and aligned with the organization's goals and objectives.

For example, an SE in an organization with goals and objectives that focus on minimizing product lifecycle duration in order to achieve a competitive advantage in bringing products to market quickly will create a TDM strategy that differs from the strategy created in an organization with goals and objectives focused on reliability at all cost. While both strategies will cover the same SSE processes presented in this book, each will seek to optimize the factors that are key to meeting the goals and objectives of their respective organizations. Generalizing process activities and relating them to one another in a hierarchical fashion can achieve a clear understanding of SSE processes and their relationships to one another. Figure 17.1-1 presents an example of this approach to organizing SSE processes. In this manner, the SE creates a structure for defining and communicating the TDM process and infrastructure that will support their project. These TDM processes form the foundation of the digital engineering environment that SE's will operate in to perform their engineering, create and share specifications and engineering artifacts, and collaborate within to optimize and tune designs and products.

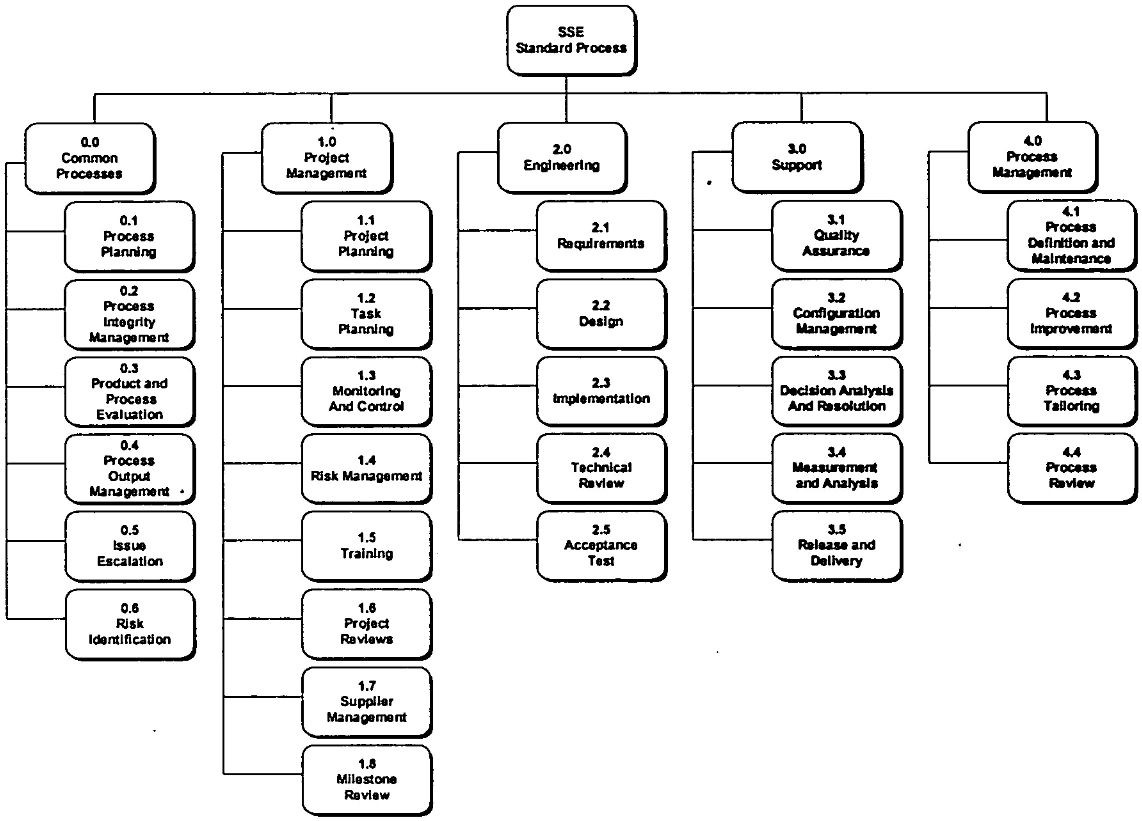

Figure 17.1-1 SSE Architecture – Here we show a sample hierarchy of SSE processes for a Space Operations company. This illustrates the broad array of processes that surround the mainstream engineering activities (2.0 Engineering column). Each of the blocks will have artifacts that document the results of the process and those artifacts must be stored and accessible through the Technical Data Management System.

17.1.1 Identify engineering lifecycle requirements for technical data

The SSE lifecycle determines the technical data and artifacts the SE must deliver or employ as they progress though the lifecycle. Today's cost and budget environment increasingly drives SSE lifecycle requirements, leading to goals and objectives focused on lean processes that are flexible, agile, and very responsive to the time pressure engineering organizations face in bringing products to market or delivering services.

Effective engineering organizations use an organized, systematic approach to the SSE lifecycle. Their engineering processes ensure that stakeholders from all phases of a product's life cycle and all impacted organizations are appropriately involved in the various phases of the development or problem resolution processes. Their processes involve customer(s) as appropriate, either through detailed interaction, or in the form of support for customer surveillance.

A tailored approach to SSE lifecycle requirements provides the flexibility for the SE to follow procedures that are appropriate to the project underway, while at the same time ensuring that all appropriate artifacts and coordination occur that will ensure success. Table 17.1.1-1 presents a sample SE tailoring guide that defines three levels of engineering, with the level of coordination increasing as one moves from level 1 to level 3. The formality and coordination of the implementation required by a particular activity is dependent on the magnitude of the activity (as defined by its visibility), approval levels, and risk (which includes safety, mission success / technical performance, schedule, supportability, and cost). Table 17.1.1-1 relates the magnitude of the project to the level of engineering artifacts and technical data that is required during execution of the SSE lifecycle.

Table 17.1.1-1. SSE Tailoring Guide - This matrix provides criteria with respect to project visibility, approval and risk that allow the SE to determine the level of rigor (i.e. tailoring) that must be applied to the development, review and maintenance of artifacts during a project's lifecycle. The level of tailoring determined here is used in Table 17.1.1-2 to determine the specific Technical Data Management requirements that must be satisfied during the lifecycle.

Level / Factor	1	2	3
	Highest factor level determines the SSE level required for a particular activity		
Visibility	Confined within a department level or lower; including customer counterparts	Confined within a company element or command level including customer counterparts	Crosses multiple company elements or command levels and/or multiple customers
Approval	Director level or below approval	Group level approval	Program level approval
Risk Identification*	Green level	Yellow level	Red level

** As defined in an appropriate risk assessment scoring process.*

Each decision factor is evaluated to one of the three levels specified in the tailoring guide. The highest factor level determines the level of SSE required for that particular activity. Table 17.1.1-2 defines the TDM requirements for each level of SSE outlined in the tailoring guide.

Table 17.1.1-2. SSE TDM Requirements - This matrix identifies specific Technical Data Management requirements for stakeholder involvement, documentation and control, etc., the SE must satisfy during the engineering lifecycle of a project. The tailoring level (1, 2 or 3) is determined from Table 17.1.1-1, based on the characteristics of the project.

Characteristic \ Level	1	2	3
Stakeholder involvement (recommend use of a checklist similar to Table 17.1.1-3)	Coordination of engineering artifacts prior to approval is generally limited to be within a department level organization, including customer counterparts	Engineering artifacts distributed for review to cross-functional stakeholders prior to submission for board/mgmt review. Some key stakeholders may be members of development teams	All key stakeholders are members of development teams. All key stakeholders are familiar with engineering artifacts prior to board/mgmt action
Product documentation and control	System engineering artifacts may not be formally documented	Formal documentation of system engineering artifacts is generally limited to that required for board/mgmt approval (if board/mgmt approval is necessary). System engineering includes an informal risk assessment and mitigation plan.	Formal documentation of all system engineering artifacts, including interim results, rationale, formal risk assessment and mitigation plan, and evident of lessons-learned application
Process documentation and control	System engineering process may not be formally documented	System engineering process is documented. Engineering process changes require formal approval	System engineering process is documented, and is under Program control. Process changes require Program or designee approval
Progress reporting	Minimal review of system engineering status	Regular informal review of system engineering status with all stakeholders	Regular formal review of system engineering status with all stakeholders

Table 17.1.1-3 is a sample checklist for use in determining stakeholder participation. This checklist is an example of the template approach that can be used to define details of the SSE lifecycle requirements as they are applied to stakeholder reviews.

Table 17.1.1-3. Sample stakeholder checklist - An "x" indicates required stakeholder involvement at each level of SSE tailoring.

Stakeholder	Level 1	Level 2	Level 3
Design engineer	X	X	X
Manufacturing engineer		X	X
Logistics specialist		X	X
Maintenance engineer	X		
Maintenance technician			X
Safety engineer			X
Flight Ops engineer		X	X
Software engineer			X
Financial analyst			
Technical manager		X	X
Program Integration			X
Reliability Engineer			X
Quality Engineer			X
System Engineer		X	X
Quality Control			X
Human Factors			X

Materials & Processes		X	X
Etc.			

17.1.2 Determine required data content and form and electronic data exchange interfaces in accordance with international standards or agreements

The technical data requirements defined in Section 17.1.1 are satisfied by project team members as they engineer the systems or components involved in each project and produce the associated engineering artifacts. The required content and form for each artifact, and the data exchange interfaces needed to share and transmit the artifacts, must be defined for each process step.

Standardizing the definition of each process allows practitioners to understand the stakeholders, inputs/outputs, and process requirements involved. This definition provides a framework for specifying the artifacts that are inputs and outputs, and the flow of data and content involved. Figure 17.1.2-1 presents a sample Standardized Process Specification that illustrates this framework.

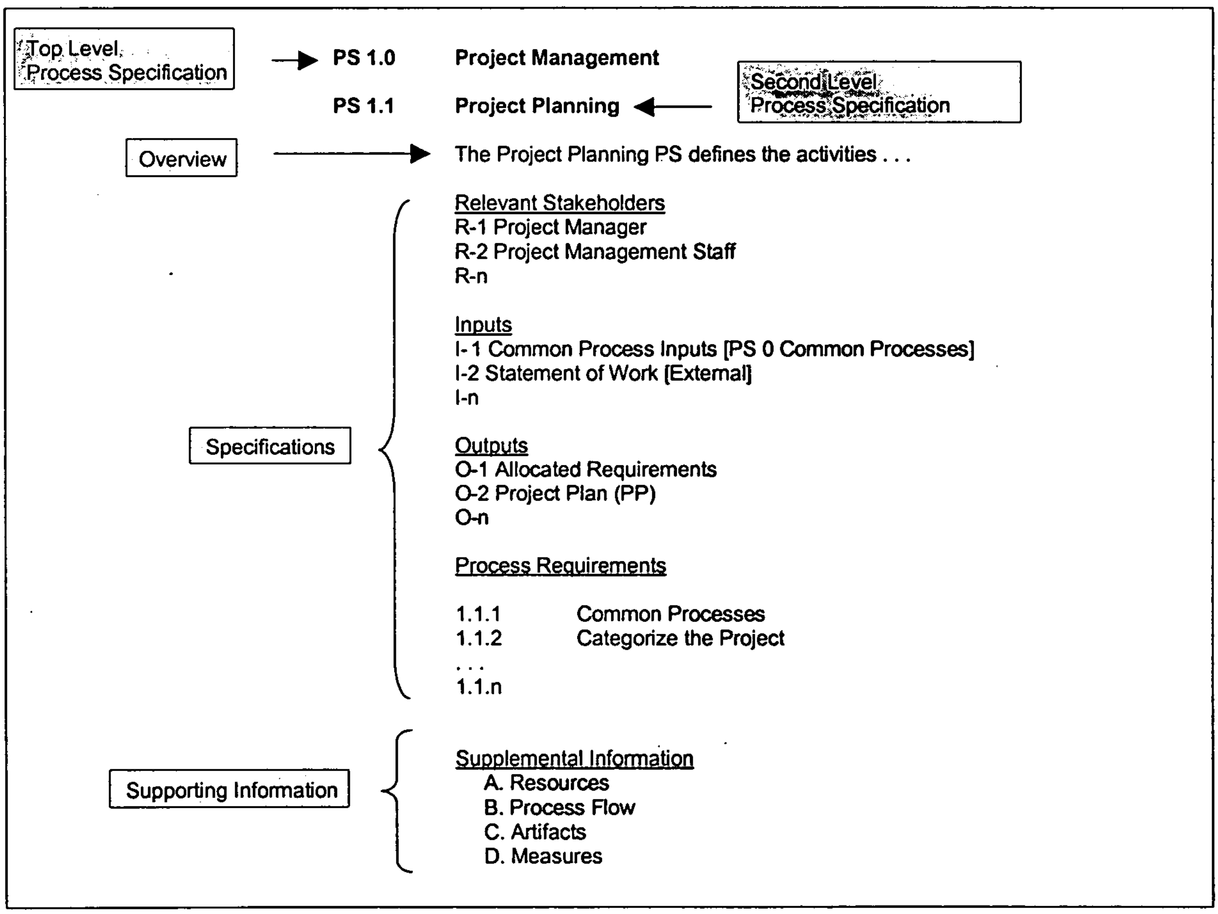

Figure 17.1.2-1. Sample Process Specification – This sample provides a standard framework for defining each SSE lifecycle process and the associated artifacts and process flows involved.

Process specifications are typically created by a Process Development Team (PDT) established for this purpose at the beginning of a Program or Project. A PDT usually consists of System Engineers and other specialists (e.g. Configuration Management specialists, Release Management specialists, etc.) with significant practical experience in their field, and with experience in constructing efficient and effective processes. Once a System Engineering process is defined, the PDT may shift its focus to monitoring and maintaining the process, or it may be disbanded and replaced by Process Improvement Teams (PITs) chartered to address specific areas where hands-on usage shows a need for optimization. Figure 17.1.2-2 illustrates the Design Process from Figure 17.1-1 specified using the standardized framework outlined above.

PS 2.0 ENGINEERING

PS 2.2 DESIGN

The Design Process Specification (PS) consists of translating detailed functional requirements into a design concept (the high level design), transforming the design concept into a detailed design, and finalizing the plans for the implementation activity.

RELEVANT STAKEHOLDERS

Definitions:

D-1. Project Team – Members of the team assembled to conduct the project as defined in the Project Plan (PP).

D-2. Engineers – Individuals assigned responsibility for designing, implementing and sustaining the engineering work products.

D-3. Additional definitions.

Responsibilities:

R-1. Project Team - Responsible for creating the High Level and Detailed Design documents, conducting Peer reviews as well as the Preliminary Design Review (PDR) and Critical Design Review (CDR), and updating the Technical Data Package.

R-2. Engineer(s) – Works as part of the Project Team to create the High Level and Detailed design.

R-3. Additional responsibilities.

INPUTS

I-1. Approved Project Plan

I-2. Approved System Requirements Specification

I-3. Additional inputs

OUTPUTS

O-1. Updated Work Request

O-2. Updated SDD, Preliminary and Detailed, as required

O-3. Additional outputs

PROCESS REQUIREMENTS

2.2.1. **Common Processes** – Perform the common process activities.

2.2.2. **Generate Preliminary Design (High Level Design)** – The Project Team analyzes the Requirements Specification, refines the operations concept, develops detailed alternate solutions and/or prototypes and develops/updates the design concept.

2.2.3. **Conduct Peer Reviews** - If required by the PP, the Project Team conducts a peer review of the high level design.

2.2.4. **Conduct a Preliminary Design Review (PDR)** – If required by the PP, the Project Team conducts a PDR.

2.2.5. Additional process requirements

Figure 17.1.2-2. A sample Design Process specification using the Process Specification framework presented in Figure 17.1.2-1.

17.1.3 Establish framework for technical data flow within the project technical processes and to or from contractors

The process specification framework presented in Figure 17.1.2-1 is supported by supplemental information that identifies the resources, process flow, artifacts and measures involved in the process. Resources are references to standards, specifications or other external sources of information that further define the process or assist in its execution. Process flows outline the sequential steps involved in executing the process. Figure 17.1.3-1 is a sample process flow for the Design Process specified in Figure 17.1.2-2 above.

To illustrate the application of this process flow consider the case of managing the FireSAT Critical Design Review (CDR step 2.2-9 in Figure 17.1.3-1). Specification of this review process must define steps covering transmittal of draft artifacts to reviewers, review of draft content, submittal of Review Item Discrepancies (RIDs), review, disposition, and incorporation of RIDs, and approval and release of the final design documentation. The FireSAT SE developing this process can take a variety of approaches, including workflow-based approaches involving serial reviews, collaborative-based approaches involving concurrent reviews, ad-hoc based approaches relying upon independent reviews and due dates, or some combination. The process decisions FireSAT makes to review documents such as the SRD, SDD and others (see project document tree in Chapter 13 and Chapter 19) become a key driver for management of FireSAT technical data.

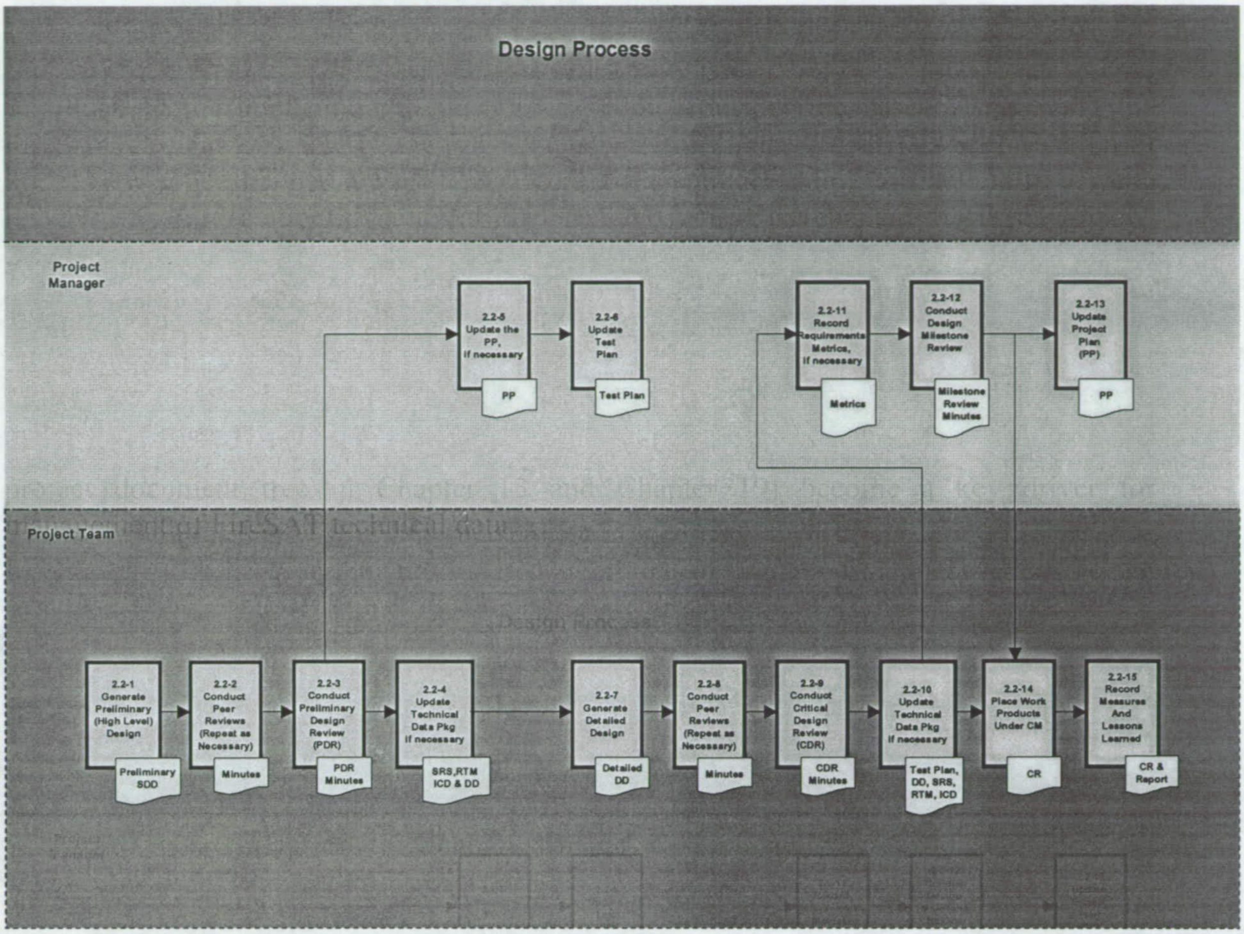

Figure 17.1.3-1. A sample Design Process flow – Each step is uniquely identified and its outputs denoted; for example, the PDR conducted in step 2.2-3 results in review minutes and triggers updating of the Project Plan in step 2.2-5 and updating of the Test Plan in step 2.2-6 to incorporate results of the PDR.

Artifacts are the products produced by executing the SSE process flow. These artifacts are the plans, specifications, drawings, models, analysis, review records and other documents, datasets and content that defines and describes the system or components being engineered and the lifecycle instance being followed. Table 17.1.3-1 shows a sample set of required artifacts for the Design Process shown in Figure 17.1.3-1. Table 17.1.3-2 defines the required artifacts for the design review package in detail.

Depending on an organization's definition of the Engineering lifecycle, the processes involved may include manufacturing and production of the system and its sustaining engineering. The output of the manufacturing and production processes is managed as a product - not as process artifacts; however, process artifacts are typically created during manufacturing and production in the form of Quality Control records, product discrepancy records, Material Review Board (MRB) records, etc. The classification and treatment of these types of artifacts is determined by the process specifications of the organizations involved.

Table 17.1.3-1. A sample set of Required Artifacts for the Design Process shown in Figure 17.1.3-1 – Each artifact is notated with the primary practitioner responsibility for producing it and with its retention requirements.

Required Artifact	Practitioner	Retention Period
Updated Work Request	PL	LOS + 2 YEARS
Updated SDD, Preliminary and Detailed, as required	PL	LOS + 2 YEARS
PDR Record/Minutes, if applicable	PL	LOS + 2 YEARS
CDR Record/Minutes, if applicable	PL	LOS + 2 YEARS
Peer Review Record/Minutes, if applicable	PL	LOS + 2 YEARS
Design Milestone Review Record/Minutes, if applicable	PM	LOS + 2 YEARS
Updated SRS, if applicable	PL	LOS + 2 YEARS
Updated ICD, if applicable	PL	LOS + 2 YEARS
Updated RTM, if applicable	PL	LOS + 2 YEARS
Prototype, if applicable	PL	LOS + 2 YEARS
Updated Test Plan	PM	LOS + 2 YEARS
Product and Process Measurements	PM	LOS + 2 YEARS
Notes: LOS is Life of System PL is Project Lead PM is Project Manager		

Table 17.1.3-2. A sample set of artifacts required for the Design Review Package – Each artifact is notated with the primary practitioner responsible for producing it and with its applicability for PDR and CDR reviews.

Required Artifact	Practitioner	PDR	CDR
Project requirements document	PM	X	
Design requirements statement	SDE	X	
Schedule preparation	PM	X	X
Design drawings	DE	A/R	X
Design specifications	DE	A/R	X
Design calculations	DE	A/R	X
Design software	DE	A/R	X
Engineering cost estimate	SDE/DE	X	X
Failure effects and modes analysis (if required)	MAE	X	X
Hazard analysis (if required)	MAE	X	X
Critical item list (CIL) impact	MAE	X	
System Assurance Analysis (SAA) (if required)	MAE	X	
System criticality impacts (if required)			
Security assessment (if required)	Security	A/R	A/R
Material Requirements List (Advance Order List)	LP&S	A/R	
Material Requirements List	LP&S		A/R
System mechanical schematic (SMS)	SDE	A/R	A/R
Electro mechanical control diagram(EMCD)	DE	A/R	A/R
Advanced electrical schematic (AES)	SDE/DE	A/R	A/R
Cable interconnect diagram (CID)	SDE/DE	A/R	A/R
Trade studies	SDE/DE	A/R	
Concept/sketches	SDE/DE	X	
Interface Control Document (ICD) changes	SDE		A/R
Environmental assessment	SDE	X	A/R
Certification Requirements (CR) Plan	SDE	X	
Notes: A/R is As Required DE is Design Engineer LP&S is Logistics Planning and Supportability MAE is Mission Assurance Engineer PM is Project Manager SDE is System Design Engineer			

Measures are the quantifiable attributes of a process that provide visibility into process performance that can result in discrete actions when defined thresholds are exceeded. Table 17.1.3-3 defines a sample metric for tracking Design Process milestone progress. The decision criteria are setup to give Project Managers and Leads warning when progress is falling behind with adequate notice to evaluate root causes and take corrective or remedial action(s). Measures are typically charted and monitored throughout the life of the project to indicate the health of the project as it moves through the SSE lifecycle.

Table 17.1.3-3. A sample measure of Design Process progress – Achievement of Major and Minor design milestones is tracked to indicate the progress being made in the design phase of the project and to highlight any risk to completing the design on time.

<table>
<tr><th colspan="3">Metric: Monitor Design Progress</th></tr>
<tr><th><u>Description</u></th><th><u>Measurement Scheme</u></th><th><u>Measures and Thresholds/Responses</u></th></tr>
<tr><td rowspan="3">Project Managers (PMs) and Project Leads (PLs) need weekly visibility into design progress to address any factors that may prevent the achievement of baselined milestones.</td><td>Design progress will be monitored via the achievement of major and minor milestones baselined to occur during weekly reporting periods.</td><td>▪ Major milestone achievement variance
▪ Minor milestone achievement variance

If a major or minor milestone completion variance exceeds 7 days (1 reporting period), evaluate root causes and identify/assign corrective and/or remedial action(s).

If a major milestone variance exceeds 14 days (2 reporting periods), report variance to all stakeholders and assemble stakeholders to evaluate corrective and/or remedial action(s) and address impacts of delay on project.</td></tr>
<tr><th colspan="2"><u>Measurement Specifications</u></th></tr>
<tr><td colspan="2">Measurement Target(s):
▪ Schedule dates and work-in-progress status of deliverables

Descriptive Measures:
▪ Milestone Type
▪ Planned Completion Date
▪ Actual Completion Date

Collection Techniques:
▪ Record planned and actual dates for milestones in Project Schedule

Calculations:
▪ Compare Planned to Actual dates to determine achievement variance (+/- days)

Results:
▪ Major milestone achievement variance (+/- days)
▪ Minor milestone achievement variance (+/- days)</td></tr>
</table>

17.1.4 Designate technical data management responsibilities and authorities regarding origination, generation, capture, archiving, security, privacy, and disposal of technical data work products

Technical data management responsibilities and authorities are typically shared among the Information Technology infrastructure provider, system operators, and users of the digital engineering environment that feeds and uses content in the TDMS. The SE's role in this arena will depend on the architecture the organization or enterprise has in place to create, manage and use technical data. Figure 17.1.4-1 illustrates a layered approach to data architecture that segregates functionality and responsibilities into discrete layers or partitions that enables the assembly of industry standard components and toolsets into a robust digital environment in a cost-effective manner.

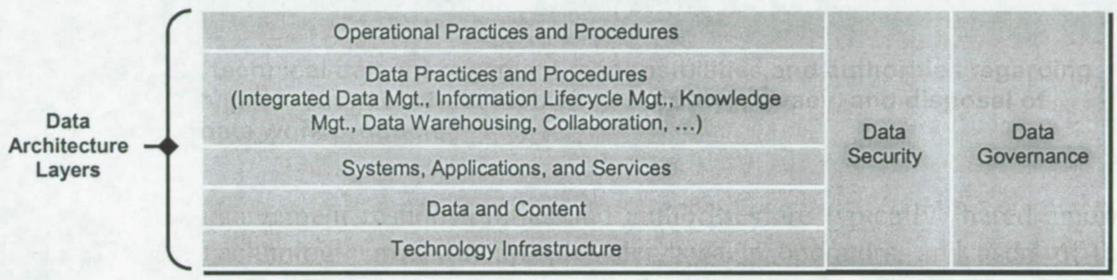

Figure 17.1.4-1. A layered approach to data architecture provides flexibility to build a cost effective digital engineering environment and TDMS.

The foundation of the architecture is the Technology Infrastructure comprised of the servers, workstations, data storage networks, communications networks, and other infrastructure elements supporting the digital engineering environment and TDMS. The next layer of the architecture consists of data, content, and metadata (data definitions) housed within the IT infrastructure. Systems, applications, and services built on the data and infrastructure form the third layer. The next layer is represented by data practices, methodologies, and toolsets such as Integrated Data Management, Information Lifecycle Management, Knowledge Management, Data Warehousing, and Collaboration, which integrate and facilitate the use and application of data and throughout the SSE lifecycle. The top layer of the architecture is comprised of Operational Practices and Procedures that tie the data, content, and technical aspects of the architecture into the organization's engineering lifecycle processes.

Spanning these layers are two key architectural elements, Data Security and Data Governance. Data Security defines the standards, structures, and techniques necessary to access, modify, and transport data throughout the data infrastructure in a secure manner. Data Governance defines the people, processes, and procedures established to institutionalize a total lifecycle view of data and content. These are essential to managing the risks to engineering projects, and form the foundation for Information Assurance practices across the digital engineering environment and TDMS.

The SE plays a limited role in the Technology Infrastructure, providing functional requirements for the systems and applications that the infrastructure supports and providing inputs on the activities that create data and content so that the infrastructure can be sized appropriate to handle the volume of data and content users will generate. The SE's role expands significantly in the higher layers that host Data and Content; Systems, Applications and Services; Data Practices and Procedures; and Operational Practices and Procedures. In these layers the generation, storage, security and disposal of engineering artifacts come into play. The specifics of an SE's role depend on whether they are a contributor, consumer, or administrator within the SSE lifecycle.

- Contributors are engineers who generate or update artifacts and work products as part of the SSE lifecycle, such as those identified in Table 17.1.3-2. Their responsibilities generally revolve around following procedures established to check artifacts into and out of the TDMS repository when creating or updating them, and classifying them accurately via the attribute data that describe them (e.g. document number, title, filename, author name, responsible department, etc.). Automated features of the TDMS will typically key off the identification, classification, or workflow of an artifact to control access, privacy and disposal. Contributors play a key role in accurately setting these attributes or executing workflows to ensure that artifacts are not compromised or corrupted via inadvertent access.

- Consumers are engineers, project leads, or other members of the project team or organization who need access to artifacts for viewing only. Consumers usually employ portals or search sites setup to access and retrieve data and content from the digital engineering environment and TDMS repository. Their responsibilities revolve around compliance with access and privacy controls and protecting data and content from inappropriate disclosure while they are accessing read only copies.

- Administrators are engineers, leads, managers or configuration management personnel whose duties involve establishing and executing data management responsibilities. The role they play is that of a data and/or system owner who must define and administer the procedures and controls that ensure the integrity, availability and quality of the artifacts and work products produced during the SSE lifecycle. In this role, SEs would define the engineering lifecycle processes that are outlined in Section 17.1.2 and illustrated in Figures 17.1.2-1 and 17.1.2-2.

A given SE will typically be both a contributor and consumer throughout the course of a project; creating artifacts either individually or as part of a team, and using artifacts created by others either as an input or as a reference. In some instances an SE may also be asked to provide administrative support, for example, by reviewing requests for access by approving those that are justified based on technical or organizational rationale.

17.1.5 Establish rights, obligations and commitments regarding the retention of, transmission of, and access to technical data items

Rights, obligations and commitments associated with access, transmission, and retention of data fall within the governance elements of the data architecture model shown in Figure 17.1.4-1. Data governance focuses on establishing policies within these arenas, and monitoring and enforcing compliance. The policies must reflect the response of the organization to a collection of factors that affect technical data retention, transmission and access, as shown in Figure 17.1.5-1. [Note to Doug: a graphic artist can improve this figure; breaking the triangle into three separate slices would be good, with each slice labeled with the intro for the set of bullets, e.g. Broadly Focused Factors, etc.]

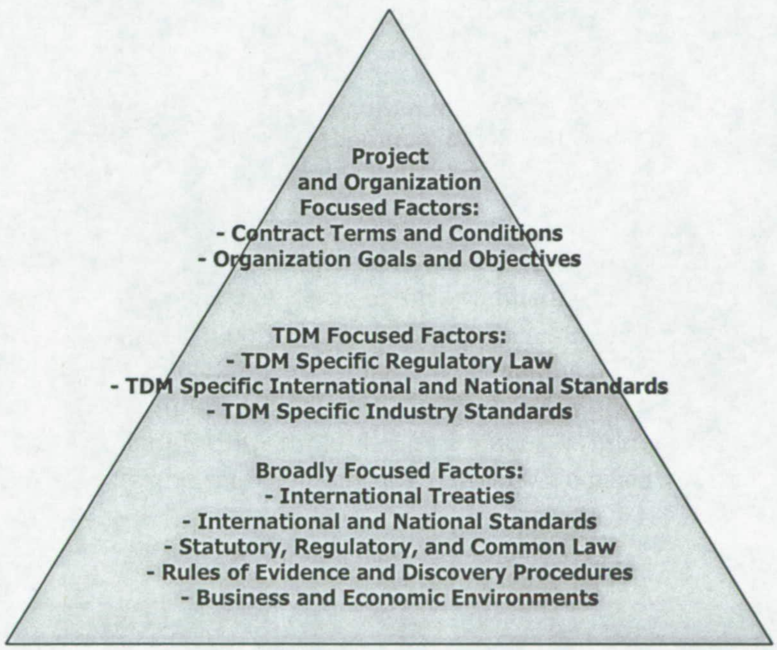

Figure 17.1.5-1. Rights, obligations and commitments associated with technical data items are driven by an array of factors, ranging from very broad to very specific. The SE defining the data governance policies and procedures that spell these out must consider the entire spectrum of factors.

The broadest set of factors is reflected in the international treaties, and the national statutory and common law forming the legal and business environment the organization or enterprise operates within. This body of statutes and rulings establishes the socio-economic environment within which the products and systems the SE produces will operate. Any litigation brought due to product or system failure, claims of negligence, patent claims or patent infringement claims occur within the context established by this legal framework. Statutes associated with product liability, tort, and the evidence discovery process (for example, the United States Federal Rules of Evidence) influence the policies that govern an organization's creation, management and destruction of engineering data and artifacts.

The next, more focused set of factors is reflected in the treaties, regulatory law and codified standards associated with the retention and control of data and content. This body of law and standards are typically focused specifically on digital content; however, key regulations affecting the SE can also be found in broader regulations. In the aerospace arena, United States government regulations controlling export and import of defense-related goods and services often come into play. These regulations, called the International Traffic in Arms Regulations (ITAR), implement United States legislation aimed at protecting U.S. national security interests and advancing foreign policy objectives.

The scope of ITAR is controlled through the United States Munitions List. This list outlines a set of goods and services subject to ITAR. The munitions list is published as Title 22 Part 121 of the U.S. Code of Federal Regulations (CFR). For example, 22CFR121.1 – General, describes 22 categories of articles that are subject to ITAR. Category IV covers Launch Vehicles, Guided Missiles, Ballistic Missiles, Rockets, Torpedoes, Bombs and Mines. Category IV, Item (d), defines missile and space launch vehicle power plants as defense articles. Hence, an organization's data governance polices and procedures associated with launch vehicle power plant engineering projects must address ITAR controls, and, for instance, their regulations precluding access to this information by foreign nationals.

The most specific set of factors are typically reflected in the contractual terms and conditions entered into by an organization or associated with a project, and the organization's goals and objectives related to its data and content. Contract terms and conditions will often specify rights in data ownership that drive how data and content must be protected or restricted on one hand, or opened up and made accessible on the other hand. Software licenses are increasing sources of rights in ownership when it comes to source code. The open source movement has spawned the General Public License (GPL), which contains terms and conditions that obligates anyone who incorporates GPL licensed software into their products or systems to specific set of requirements for copying, modifying and redistributing the works.

Organizational goals and objectives reflect the most specific drivers behind an organizations data governance policies and procedures. They embody the attitude and strategy an organization takes in controlling and managing data and content. For example, some organizations may elect to manage key pieces of data and content as trade secrets – certain critical facets of a design for instance. These organizations would implement extremely tight controls for this key data. A different organization might instead choose an alternate approach by patenting the design and licensing it to all interested parties; in effect publishing the concept and selling the design details to anyone willing to negotiate acceptable compensation.

Regardless of the factors that drive data governance policies and procedures to a specific point, they need to be effectively communicated to the project team personnel who must adhere to them, and they must be adequately reflected in appropriate system controls within the digital engineering environment and TDMS. Section 17.3.3 address this in detail.

17.1.6 Establish strategy for relevant data storage, transformation, transmission, and presentation standards and conventions to be used in project or program policy, agreements, and legislative constraints

The strategy for data storage and access (transformation, transmission, presentation, etc.) is key to implementing the digital engineering environment and its supporting TDMS. The strategy in this area must be carefully considered; all subsequent implementation actions reflect this key decision. Key factors in the decision involve cost, flexibility, responsiveness to change, and risk.

Cost involves initial acquisition and installation as well as subsequent maintenance and upgrade costs over the lifetime of the system. Flexibility involves the ability to upgrade all or parts of the system as technology evolves and new capabilities become available in the market (e.g. new content visualization tools and techniques). Responsiveness to change involves the ability to quickly modify or enhance the system to meet changing business requirements (e.g. moving from a single contract line of business to a multi-contract line of business). Risk involves an array factors ranging from usability, operability, supportability, scalability (any many other "ilities"), to technology obsolescence and failure of technology suppliers to deliver or keep up, to inadequate alignment of technology and business strategies, to name a few.

The SE involved in the setup and provisioning of a digital engineering environment and associated TDMS must work closely with software system architects, IT subject matter experts, business analysts, and other parties to analyze and evaluate alternative strategies, and decide on the strategy that makes the most sense for their organization and their situation.

Figure 17.1.6-1 illustrates one possible strategy. This strategy entails a common logical data and content repository that is physically distributed among the organization's elements and project locations. What this means is that implementation will result in two or more physical repositories located in data centers (or supported by services providers) in different physical locations the organization chooses. A common logical repository means there is communications and synchronization of data and content between the multiple physical repositories. This synchronization could occur at a variety of levels, ranging from the physical level where content is duplicated or replicated among the physical repositories, to the application level where the applications provide the ability to store and access data in any one of the physical repositories, all the way to synchronization at the metadata (data definitions) level where a common metadata repository holds information about each piece of data, including its authoritative location within the set of repositories and the location of all its copies or replicas.

The strategy also entails partitioning the software tools that make up the digital engineering environment and the TDMS into various layers, with the tools interacting via the data and content stored in the logical data repository, and an enterprise-wide messaging bus (not shown) that allows tools to communicate among each other when necessary. This strategy "loosely" couples the tools and the data from the perspective that the data can exist independent of any particular tool.

The strategy outlined in Figure 17.1.6-1 aims to minimizes lifecycle costs by favoring tools that are based on non-proprietary or open formats. This facilitates competition and minimizes proprietary vendor lock-in. It also aims to minimize upgrade costs over the lifespan of the system by enabling the swap out of higher cost tools with lower cost tools (consistent with the delivery of the necessary functionality, supportability, and performance) as competition drives down price points, without costly data and content migration from one proprietary format or data structure to another. Flexibility is achieved by enabling additional physical locations to be added or subtracted as the organization's needs dictate (since the architecture is designed to support this from the get go), as well as enabling the addition and removal of tools as needs dictate. Responsiveness is enabled through the loose coupling of tools and data, the adoption of open or industry standards, and the use of enterprise-scoped metadata that provides visibility into data and content as it is used across the organization. Risk is minimized from multiple perspectives: first, through the diversification and redundancy that can be achieved among multiple physical repositories with respect to system failure at a single location, second, through the diversification that can be achieved by appropriate provisioning of tools from multiple vendors (risk, however, can actually increase due to integration and supportability factors if the number of vendors grows large and unwieldy, or they are not properly managed), and third, obsolescence is minimized by enabling technology upgrades of various components without wholesale replacement of the entire system.

Variations on the strategy outlined here are possible, and numerous other strategies can be devised as well. The ultimate challenge of the SE and the support team implementing a digital engineering environment and its underlying infrastructure is to devise a strategy that satisfies the goals and objectives of the organization, meets the needs of the project teams that depend on it, and can keep abreast of the constantly changing landscape that organizations must deal with over time.

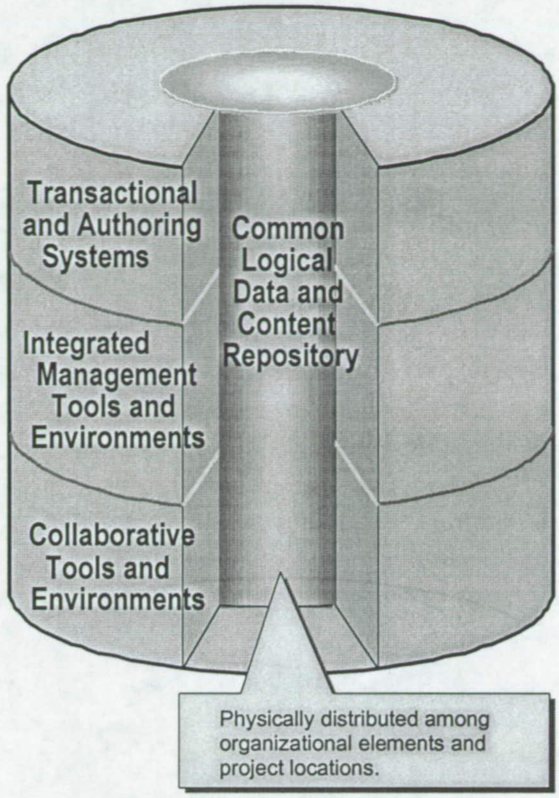

Figure 17.1.6-1. A data storage strategy based on a common logical data and content repository that is physically distributed provides many benefits. Lifecycle costs, flexibility, responsiveness to change, and risk, all factor into development of the data storage strategy.

17.1.7 Describe strategy for the methods, tools, and metrics used during the technical effort and for technical data management

The strategy for data storage and access outlined in Chapter 17.1.6 cannot be effectively constructed without consideration of the tools envisioned for creation, management and use of data and content. The strategy presented for illustration purposes considered methods and tools within the context of data storage and access to derive an integrated strategy.

Data storage and access is difficult to impossible to deliver independent of methods and tools. Hence, any effective method and tool strategy must also address toolset evaluation and selection. Toolset selection is heavily dependent on the style of the organization. It typically begins with the organization's preferences and beliefs in developing its own tools (make), versus purchasing COTS tools from software vendors (buy), versus buying COTS and modifying them to its own unique requirements and preferences (modified COTS).

Once a make vs. buy decision has been made, toolset requirements in some form must be defined. Toolset requirements can range from formal functional requirements, to checklists of toolset "musts" and "wants", to a loosely assembled collection of vendor marketing materials that outline the feature of various products. Requirements definition also reflects the style and practices of the organization. Structured and formalized definition processes are recommended, since ad hoc, informal, approaches tend to produce results that are typically subjective and dependent on the composition of personnel involved and the biases and preferences they bring to the table.

Once toolset requirements are defined, any number of decision making processes can be used to determine the selection, ranging from a decision of one or more organizational executives, to formal decision analysis techniques such as the Kepner-Tregoe Decision Analysis process, SWOT (Strengths, Weaknesses, Opportunities, and Threats) analysis, decision tree analysis, to group decision techniques such as unanimity, majority vote, range-voting, multi-voting, consensus building, or the step ladder technique. Regardless of the process, the outcome of the selection process is the basis for implementation and deployment of the digital engineering environment and TDMS.

In certain settings the specifics of the selection process are formally established. In situations where United States Federal acquisition is involved, Federal Acquisition Regulations (FAR) outlines processes for contracting; FAR Part 15 Subpart 3, for example, defines the procedure for selecting sources of products that represent the best value. In other situations, the techniques associated with the make vs. buy decision are applicable. In many instances, the alternatives are structured in a manner such that the details of the approach are embodied in a single decision making process. All decision-making processes ultimately come down to some form of evaluation of alternatives against criteria or requirements. Whether the process is deterministic, heuristic, or subjective, requirements form the basis of the decision making process. It is often tempting to skimp on requirements definition, or to entirely short cut it. To do so dramatically increases the risk that the digital engineering environment and TDMS will fall far short of its intended goals, or fail entirely.

17.1.8 Prepare training strategy for appropriate technical team members and support and management personnel in the established technical data management strategy and related procedures and tools

The training strategy for the digital engineering environment and TDMS must address engineering project team members, functional and IT support personnel, and management personnel in all domains involved in the SE lifecycle. The strategy must address:

- Training needs in terms of necessary knowledge and skills, expected levels of proficiency, and experience required.
- Certification methodologies and graduation criteria that will document and validate knowledge, skills and proficiency - such as certification testing, stand boarding, or qualification checkout.

- Techniques that will be used to delivery training - such as in person lecture, remote video conferencing, computer-based, one-on-one, or train-the-trainer.
- Outlines that identify training content by course or topic, which enable specialists to build training content that meets the needs of the organization.
- Training course relationships and training pre-requisites that establish criteria for attendance.
- Training support, including subject matter expertise and consultancy.
- Criteria for retraining when personnel performance levels fall below specific thresholds.

17.2 Collect and Store Required Technical Data Artifacts during the Engineering Lifecycle

The SE lifecycle for projects undertaken by the organization generates the artifacts that are stored in the TDMS data and content repository. The digital engineering environment provides the authoring and tools used to create, modify and use these artifacts. Tools such as Computer Aided Design (CAD) systems to generate drawings and perform kinematic analysis, finite element systems to create and analyze models for structural, thermal, and fatigue analysis, and numerical analysis packages are some examples of the many tools the SE will typically deal with.

17.2.1 Identify existing sources of technical data artifacts that are designated as outputs of the common technical processes

The ASE lifecycle outlined in chapters x – y, and the organization's process specifications that implement it (see Chapter 17.1.2) define the specific data artifacts that will be generated during execution of the lifecycle. The project planning and estimating phases will identify at a high level the engineering content that must be generated, including updates to any existing engineering artifact baselines that are relevant to the project at hand. These baselines may represent the as designed or as-built configuration of hardware, facilities, or systems that the current project relies on, augments, or interfaces with, or may represent items or systems that must be decommissioned or demolished to make way for the current project. In certain cases these systems may be very old and their associated engineering may not even reside in electronic form.

It is important for project managers and leads to consider the form and format of any existing baselines that are targeted for update with respect to the tools and capabilities of the organization's digital engineering environment and TDMS. Artifact baselines (for example CAD drawings, 2-D and 3-D engineering models, simulations, etc.) created in earlier versions of the toolset, or in tools that are no longer part of the digital engineering environment, may require significant cost and effort to convert to the current version, or may even require recreation using the current toolset. This potential data translation effort must be evaluated and properly accounted for in project planning and costing in order to avoid unpleasant surprises when engineers go to use or update these artifacts.

17.2.2 Collect and store technical data in accordance with the technical data management strategy and procedures

The creation or capture of content will typically take a multitude of forms in the digital engineering environment, depending on the artifact involved, its authoring or creation toolset, and the context involved. Tools that are native elements of the digital engineering environment and are integrated with the TDMS will enable System Engineers to generate new content objects within the toolset and check them into the TDMS as part of the tools user interface. Using integrated toolsets, existing objects can easily be checked out of the TDMS, modified, and checked back in under a versioning scheme that is setup for the situation at hand.

The System Engineer may use a number of support tools to generate or capture content that may not be integrated into the digital environment as the core tools typically are. The artifacts and content generated by these tools require alternate methods to move them in the repository. Some examples would be digital cameras used for photo documentation purposes on site surveys, or satellite imagery purchased from a commercial source to support engineering analysis. In these cases, the data and content will typically be moved into the TDMS via general user interfaces provided by the TDMS to navigate within it's content structures, and to import, check out, or check in content. In some cases, general-purpose data capture pipelines may be available to move content into the TDMS from any accessible location (local computer hard drive, shared file server, web site, etc.).

Another potential source of technical content are the data deliveries made by partners, subcontractors, or affiliated parties involved in the engineering project. Submission of these types of data sets will occur per the contractual or teaming arrangements established for the project. The arrangements can range from physical shipment of electronic media (content on CDs, DVDs, tapes, etc.), to basic file transfer processes using mechanisms such as File Transfer Protocol (FTP) or secure FTP, all the way to formal structured data transmission interfaces based on industry standard or custom data exchange structures implemented for this purpose. Standard transfer mechanisms have been established in a number of arenas, including the electronics industry, manufacturing, and aerospace. Several examples of these include:

- ISO 10303 – Industrial automation systems and integration – Production data representation and exchange, The International Organization for Standardization, www.iso.org [also known as Standard for the Exchange of Product model data (STEP)]

- EIA-836 – Configuration Management – Data Exchange and Interoperability, Government Electronics and Information Technology Association (GEIA), www.geia.org

- IPC-2578 – Sectional Requirements for Supply Chain Communication of Bill of Material and Product Design Configuration Data – Product Data eXchange (PDX), Institute for Printed Circuits, www.ipc.org

17.2.3 Record and distribute lessons learned

Capturing and applying lessons learned from previous iterations of the engineering lifecycle, and from projects preceding the current, is essential to the meeting the process improvement goals and objective of most organizations. The SSE process architecture presented in Figure 17.1-1 covers this in process 4.2 – Process Improvement. Process Improvement should establish a formalized means to identify and capture lessons learned during the closure phase of all projects, as well as the investigative and root cause results of anomalies, discrepancies and failures.

A database or repository is an effective way to capture and organize lessons learned. Integration of the database or repository into the project team's digital environment is key to ensuring that lessons learned, rules of thumb, and the experiences of previous projects are accessible to team members and readily applied to the tasks at hand.

While internal lessons learned are vital to process improvement, lessons learned from entire industries are available in the form of group, national, and international standards. These standards reflect the cumulative expertise and lessons of industry and academia that can be leveraged and applied to improve an organization's engineering processes. Some notable programs applicable to system development are outlined below.

- ISO 9001 – The International Organization for Standardization defines standards for quality management systems within its ISO 9000 family of standards. These standards address how products are produced, and are intended to ensure consistent business processes are being followed that lead to quality products. ISO 9001 defines process requirements, and ISO 9004 provides guidelines for process improvements.

- Lean Six Sigma – Six Sigma is a business improvement methodology developed at Motorola in 1986 aimed at defect reduction in manufacturing. The Lean variation of Six Sigma reflects the mindset required for improving service oriented processed that are time or cycle based. Although sigma denotes the measure of standard deviation (applied to defects in this case), the heart of the program is a Define, Measure, Analyze, Improve, and Control (DMAIC) procedure for improving processes.

- Capability Maturity Model Integration – CMMI is a system development methodology that describes the essential elements of effective processes; in effect the lessons learned from a vast collection of experiences of system engineering practitioners. The Software Engineering Institute, in collaboration with members of industry and government, developed CMMI. CMMI describes effective processes in 22 areas covering the entire spectrum of system engineering, construction and maintenance. Each area describes progressively effective practices that lead organizations following its strictures to be appraised as operating on a 1 to 5 scale with respect to the effective processes.

- Information Technology Infrastructure Library – ITIL is a framework of industry best practices covering management procedures associated with IT system operations. While ITIL does not address system development per se (it assumes that systems are in place and operational), it does provide best practices associated with operating installed systems, managing infrastructure and systems, and supporting and delivering IT services.

17.2.4 Perform technical data integrity checks on collected data to confirm compliance with content and format requirements and identifying errors in specifying or recording data

The primary data integrity checks against collected or captured data and content must occur during the collection process. These checks must ensure the data and content conform to the format standards established for the type of artifact involved, and the metadata describing the artifact contains the mandatory information needed to store, manage, and use the data or content. In addition, content checks may include certifications with respect to ownership rights (e.g. public domain content, licensed content, or third party proprietary content), marking of the content (e.g. classified, restricted, proprietary, copyright, non-disclosure), or scanning of the content for Digital Rights Management (DRM) restrictions. The capture process may also involve watermarking of the content or applying other DRM controls to enforce ownership of the content by the organization involved.

Any data or content that fails the integrity checks should be rejected to the submitter for correction or rework, or should be moved to a holding area to be reprocessed according to procedures established for this purpose. Once data and content has been collected and stored in the TDMS, internal audit procedures should be established to spot check or randomly audit data and content to ensure that integrity processes procedures are being followed and are effective.

17.2.5 Prioritize review, and update technical data collection and storage procedures

In most organizations the technical data collection and storage procedures associated with the SE lifecycle will be one part of a larger set of policies and procedures that defines and implements the lifecycle. Review and updating of these procedures should be included in the management of the entire set. A formal requirement for periodic review of each policy and procedure should be documented as part of the organization's formal processes.

The requirement should establish the basis and criteria for review and update of policies and procedures. The criteria should address the types of changes the review must solicit (typographical, clarity of content and instruction, actual practice experience, etc.), the means of review (tabletop review, distributed review (via email, wiki's, etc.), continuous review (via electronic suggestion boxes, etc.)), and the update approvals required tied to the nature of the changes involved.

An example of this might be an annual review tied to the original release date of the policy or procedure, conducted by the department manager identified as the owner. The review process might require the owner to maintain a list of Subject Matter Experts (SMEs) across the topic(s) the policy or procedure addresses, with the requirement to solicit via email any material changes or enhancements required within the policy or procedure. The process might enable typographic changes to be incorporated with the sole approval of the management owner, require content and instruction type changes to be approved by the next higher level of management, and require process changes to be approved by affected process owners within the organization. Another approach could involve the posting of a policy or procedure requiring review on a wiki-based internal web site, followed with assignments to specific parties to update the policy during a given review window. Upon closing of the review window, an approval window could open where approvers view the changes and signoff on them online. A third approach might involve electronic workflows triggered by annual review timers that route policies and procedures to identified parties for review, updating (if required) and release.

17.3 Maintain Stored Technical Data

Once engineering artifacts are created, reviewed and baselined, they are stored in the Technical Data Management System. Sound Configuration Management (CM) practices create and manage baselines through a documented release process. Updates to artifacts are tracked and managed through a revision control scheme. Any iteration of the SSE lifecycle can result in some or all of the baselined artifacts being revised and re-released.

The System Engineer tasked with establishing a TDM process and infrastructure for a major project has a wide variety of choices today to build repositories for engineering artifacts and business processes to handle engineering release and revision.

17.3.1 Review and release system engineering artifacts

In the TDM framework we have been building in this chapter to illustrate the concepts and practices involved, the requirements for engineering artifact review and release are covered in the process specifications illustrated in Section 17.1.2. These specifications will outline the requirements the process must satisfy, while process flows will detail the specific tasks and steps involved.

In the digital engineering environment, process flows are defined and executed in the form of electronic workflows. Workflows can be setup using dedicated workflow engines and toolsets, or setup using workflow features of the artifact repository being used to store and manage the data and content involved. Additional capabilities are available in the form of the Business Process Execution Language (BPEL) that enables process models to be created which are executable.

BPEL is an orchestration language published by the Organization for the Advancement of Structured Information Standards (OASIS). Implementation is based on industry standards such as the eXtensible Markup Language (XML) and the eXtensible Stylesheet Language for Transformations (XSLT), and BPEL toolsets are available from a variety of vendors. BPEL provides an array of constructs to execute flows such as sequence, if-then-else, if-else, while, and other flow related commands.

The choice of a workflow approach or a BPEL approach will often be driven by the scope of the review and release flow. Flows that are contained within a single organization using its own digital design toolset will typically be implemented through the workflow features of the toolset. BPEL on the other hand is designed to define the interactions and transitions that need to occur during a business process so that the process can be assembled and executed as a collection of web services.

A web services approach lends itself to process flows that span multiple organizations with different digital environments. Each organization can integrate its engineering environment into the flow by creating web services that encapsulate and interface its interaction within the review and release flow. Due to its standards-based nature, BPEL is well suited to implement process flows across organizations, companies, and agencies that employ disparate Information Technology (IT) infrastructures.

Figure 17.3.1-1 illustrates a conceptual engineering artifact review and release flow that could be implemented using either workflow or BPEL. This flow is presented as a Sequence Diagram using the Unified Modeling Language (UML) that shows the interaction of the review and release processes. The sequence diagram shows each participant with a lifeline (running vertically), the messages that are targeted to and from the participant (running horizontally), and in certain cases the parameters that the messages will carry.

The sequence diagram here models a simplified, success-oriented, scenario. The models for a robust, production process must cover all scenarios and incorporate error processing, exception handling, iteration through various steps, and the many other details involved in production processes. Some of the details the SA must deal with when implementing a review and release process revolve around topics such as identification schemes for artifact revisions, criteria to determine who the reviewers are and who the approvers are, the mechanics of the notification and comment incorporation process, and whether artifacts will carry effectivity - and if so what type (date effectivity, lot effectivity, serial number effectivity, etc.).

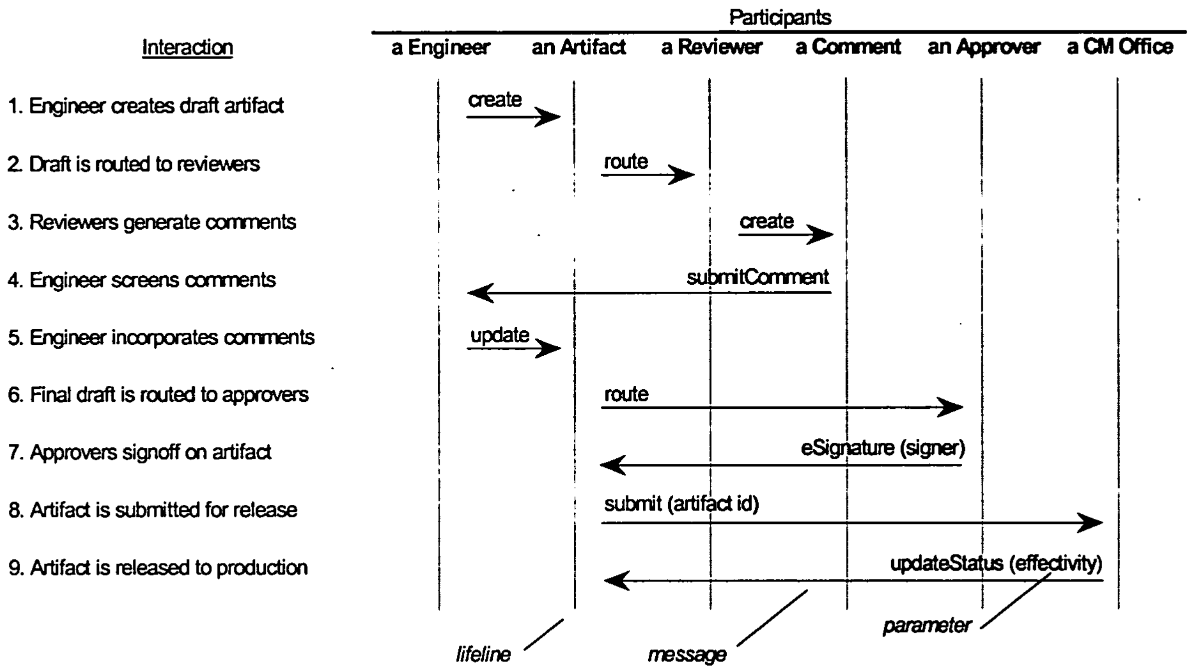

Figure 17.3.1-1. A sample Engineering Review and Release Process expressed as a UML Sequence Diagram. Each participant is listed across the top. The interaction between participants is specified as messages to and from each.

17.3.2 Update and revise system engineering artifacts

Many processes in the technical data management arena share common underpinnings. Updating and revising system engineering artifacts embodies nearly every process step involved in reviewing and releasing artifacts, with the distinction being an update focus versus a creation focus. This difference can be huge with respect to the attention focused at each step, the engagement of personnel at each step, the rigor applied, etc., however, from the TDMS perspective, the processing of the artifacts follow a nearly identical course.

In cases such as these, a Service Oriented Architecture (SOA) provides advantages over alternatives in its ability to easily construct processes and flows from "libraries" of standardized services. The SOA advantage is these services can be abstracted or generalized, and derivative process flows can be created easily with very low cost and effort. Figure 17.3.2-1 illustrates a conceptual engineering artifact update and revision flow. This flow parallels the artifact review and release flow in Figure 17.3.2.1-1, with only minor changes to reflect an update verses creation. Implementation of this flow using a BPEL approach would be very straight forward using the services in hand for the review and release process.

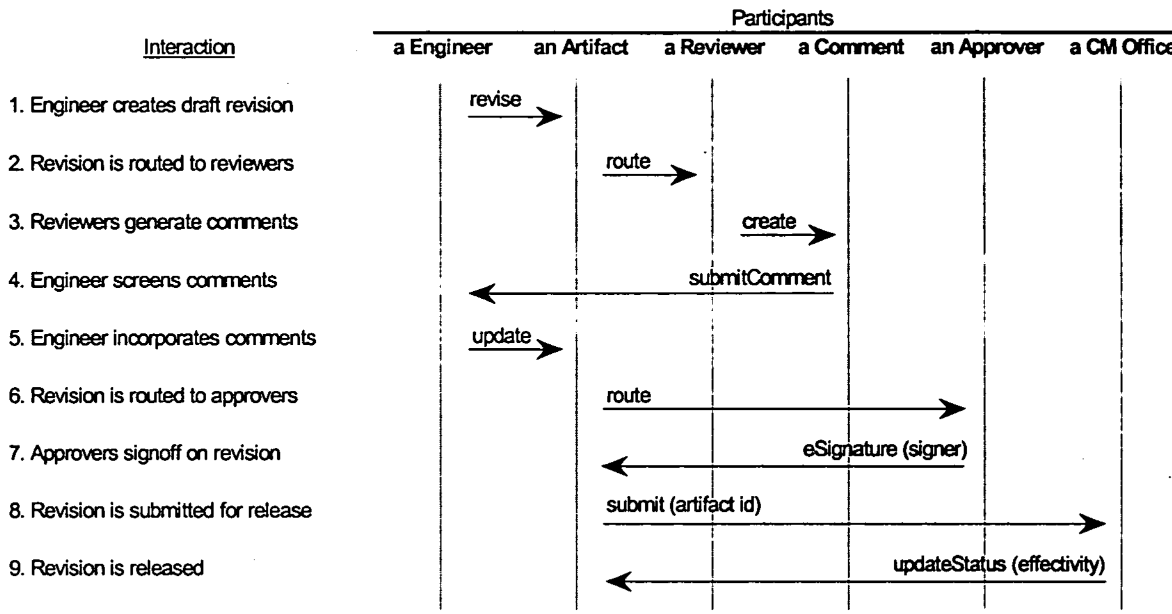

Figure 17.3.2-1. A sample Engineering Update and Release Process expressed as a UML Sequence Diagram. This is nearly identical to the process flow in Figure 17.3.1-1, and could easily be implemented using an SOA approach.

17.3.3 Manage databases to maintain proper quality and integrity of the collected and stored technical data and to confirm that the technical data is secure and is available to those with authority to have access

Managing the TDMS and its databases requires focus in two main areas: first, on the users who are authorized to access the system, and second, on the data and content the system is managing. The start of operations (the go-live of the system) marks the beginning of the system management process, but this does not occur without significant preparation and planning. Go-live requires the initialization of many system structures. Some of the key initialization tasks involve:

- Setting up user accounts
- Setting up groups, roles and permissions
- Setting up storage schemes and structures
- Setting up access controls
- Loading initial content and data

The user registration process must be in place for go-live as either a system feature or a supporting process. For a TDMS with a signification numbers of initial users, it is often more effective to preload the initial set of user accounts to eliminate user registration as a bottleneck at go-live. This requires the project team to assemble user account data as a pre-requisite to go-live, and for the development team to build and run a one-shot job to populate user account structures within the system. When the number of initial users goes beyond several hundred, the benefits of having accounts in place at go-live outweighs the cost in effort and coordination needed to do so.

Groups, roles and permissions are essential features for any TDMS whose mission goes beyond narrow, specialized, data capture and management. Groups, roles and permissions are generalized capabilities that must be employed by system administrators to create specific instances that will control the system at go-live. Setting up groups and roles and loading user accounts into groups can be very time consuming if the number of groups and users is large. Mapping permissions to roles can also be time consuming if the role and permission scheme is complex. In situations such as these, pre-loading user accounts is mandatory since without fully configured groups, roles and permissions at go-live the system will be inoperable. Some form of automation to support administrators (either in the form of one-shot system updates or an administrative interface that streamlines the configuration process) is essential for systems that must handle hundreds or thousands of users.

The storage scheme used by the TDMS is determined by its design. Any robust TDMS will provide a flexible, extensible, scheme. Storage schemes and structures for go-live are driven by the initial content and data load, and the projected expansion post go-live. If, for example, content is stored in a cabinet/folder scheme, the initial set of cabinets must be established prior to go-live, as well as an initial set of folders capable of holding go-live content. If the folder-naming scheme is tied to content, the scheme must be setup to be immediately extended as additional content flows into the TDMS. Again, administrators must setup the structures, and if extensive, they may require some form of automation to complete the task in a timely manner.

TDMS access controls are can be implemented in many forms under one of a half dozen or so access control models. A popular control model employs Access Control Lists (ACLs) or similar structures that associate users or groups of users to specific instances of content or collections of content (e.g. all content within a given folder). Many access control schemes provide an inheritance capability so that higher-level ACLs can waterfall down to lower levels. As with groups and roles, access controls must be in place at go-live.

17.3.4 Perform technical data maintenance as required

Operation of the digital engineering environment and the TDMS should be in accordance with a Maintenance and Operations Plan (MOP) created by the organization for this purpose. The MOP defines key organizational, procedural and contingency structures that ensure the health and reliability of the TDMS. Key content within the MOP covers:

- Operational Roles and Responsibilities – ORRs define who does what to operate the system. Some examples of groups that are typically called out include:

- Network Communications: responsible for setting up access to the TDMS through the WAN or LAN, and monitoring the network traffic to and from the TDMS.
- Infrastructure Services: responsible for operating the servers, data storage farms and application services that comprise the TDMS, and monitoring system and TDMS health and performance.
- IT Security: responsible for responding to system threats (e.g. intrusion by hackers, denial of service attacks, etc.), and monitoring system security controls.
- IT Service Desk: provides a single point of contact to the user for all service requests and problems; responsible for working with users to resolve incidents caused by know errors with know solutions, and for escalating all other incidents through the TDMS problem escalation procedure.

- Operational Processes and Procedures – OPPs are essential to providing consistent and reliable TDMS services. OPPs define the specific steps personnel involved in TDMS operations will use to accomplish tasks and respond to foreseeable situations. Documented procedures eliminate ambiguity and enable rapid response to real time situations that can adversely affect TDMS availability. System startup/shutdown procedures and system backup procedures are examples.

- Operational Measures and Metrics – OMMs provide the pulse of the TDMS. Metrics must be designed to support the needs of each ORR, and today, many COTS system management solutions are available that provide real time monitoring, alerts, and the measures and indices that form the OMMs. Measures such as system uptime, system availability, network bandwidth use, network latency, average and peak response times, and problem resolution response time are just a few examples of the metrics required to monitor the health of a TDMS.

- Service Level Agreements – SLAs are agreements between providers and consumers of services with respect to levels of service by type of service. SLAs can be either internal or external focused. TDMS external SLAs typically focus on user-oriented concerns such as performance (e.g. average and peak response times for standardized interactions), availability (e.g. available greater than 99.9% of standard operating hours), and incident resolution (e.g. reply to problems received via email in less than 6 hours). TDMS internal SLAs typically focus on infrastructure and system-oriented concerns such as recovery (e.g. system recovery from backup tapes in less than 12 hours), troubleshooting (e.g. high priority problem tickets will be owned and investigated within 1 hour), and maintenance (e.g. normal maintenance outages will be less than 3 hours in duration, occur between 00:00 and 06:00 hours, not more than once per month).

- Problem Management, Escalation and Tracking – Incidents reported by users to the Service Desk can often be resolved by tracking know errors and solutions (e.g. a user reports they cannot login successfully and they are typing their password correctly; the Service Desk agent asks them to check their caps lock on their keyboard since passwords are case sensitive; the user reports that caps lock is on, turns it off, and is now able to login). Any incident that cannot be resolved by the Service Desk agent is documented as a problem and escalated within the TDMS support organization. Procedures for tracking, escalating and managing problems are a key part of the MOP. Organizations that operate many systems will typically define problem resolution procedures in documents dedicated to this topic. In this case, the MOP should reference the standardized procedure and outline any unique characteristics of the TDMS that may affect the procedure (e.g. instruct Service Desk agents to always include the name, type and format of any content files associated with TDMS problems).

The MOP outlines the procedures for operating and maintaining the TDMS per se. The content held within the TDMS also requires maintenance. The nature of the content itself and its volume determine the specific support structure and procedures for maintenance. Maintenance is generally focused in two arenas, 1) the content files themselves and 2) the data attributes describing each piece of content. Maintenance also occurs at both a physical level and at a logical or administrative level. Maintenance at the physical level occurs against the servers, disk drives, file systems and data base management systems that support the TDMS. Maintenance at the logical or administrative level occurs against the TDMS structures and constructs it provides to grant and control access and facilitate use of the system. Logical or administration level maintenance always takes place through the TDMS itself or a toolset it provides for this purpose.

Most TDMS designs store content within a computer file system. Maintenance of the TDMS content thus falls within the practices and procedures associated with file system or file share maintenance. Key file system maintenance activities include monitoring file system fragmentation, taking proactive and retroactive steps to address fragmentation, monitoring free space and expanding free space as needed to accommodate content growth, and monitoring file system access rights to ensure granted rights match the rights specified in system TDMS design and operations specifications. Monitoring of system events logs and file system metadata are also key activities that ensure access to the TDMS' underlying content files is secure and controlled.

Most robust TDMS designs store content attributes in a relational database management system (RDBMS). In this case, maintenance of attribute data falls within the practices and procedures associated with database maintenance. Key RDBMS maintenance activities include managing the resources supporting the database (disk space, system memory, system bus configurations, etc.), ensuring any statistics that are required for query and access path optimization are collected or updated on a regular basis, and tuning the performance of the RDMBS to assist in meeting the Service Level Agreements associated with system performance, responsiveness and availability.

Content administration (maintenance at a logical level) is primarily focused on controlling and monitoring access to prevent content from being used or accessed inappropriately. In certain setting the access of content by unauthorized parties has significant ramifications; government classified information and export controlled information are prime examples. The challenges associated with content administration hinge on the dynamics of the TDMS user community. A stable community having access needs that are static over time represents a relatively simple administration task. Once setup, the access controls (groups, roles, permissions, etc.) require few changes and administration is basically a monitoring task. A dynamic setting in which users come and go frequently and access needs constantly change poses the most challenging administration task. In cases such as these, the automation provided by a CURF-type system enables user accounts to be created and destroyed or de-activated with a minimum amount of effort, and allows requests for changes in access to be processed using pre-defined workflows that streamline administration and provide standardized audit reports.

17.3.5 Prevent stored data from being used or accessed inappropriately

Access controls in the digital engineering environment and TDMS must be configured and implemented properly to prevent data and content from being used or accessed inappropriately. Their features must be configured to achieve the desired combination of openness, restrictiveness, and maintainability. The design of the TDMS determines the access controls it provides the SE, and as such, is often a deciding factor in toolset selection for an engineering organization. The TDMS access control model, whether it is based on a mandatory, discretionary, role, or capability approach, must support the requirements of the organization's data security policies and architecture.
Figure 17.3.5-1 shows a typical set of controls that an SE may be using to manage access to engineering artifacts. This example is based on an implementation of a discretionary access control model that allows "owners" of a piece of data or content to alter its access controls at their discretion and/or transfer access controls from one piece of data or content to another through an inheritance scheme.

Figure 17.3.5-1 is in the form of an annotated UML Class diagram outlining the access control features available to system administrators and data owners. A fundamental entity is the user, who is an authenticated subject interacting with the system. Users can be organized into groups that make administration of access controls easier. Each group has many users, and each user can be in many groups (a many-to-many association). Central to this example is the Access Control List (ACL). Each ACL has one or more groups or individual users called out, along with one or more rights or privileges (such as read access, write access, the ability to version the object, or the ability to delete the object, for example).

In this example, ACLs provide control when they are assigned to instances of data, content, tools, or services (i.e. Technical Data Resources) managed or provided by the system. Each resource is associated with an ACL that controls access to it, and operations upon it (e.g. versioning it). A default ACL (predefined by the system or by a system rule – e.g. inherit the ACL from the folder the object is stored in) could be associated with any object that the owner or administrator fails to explicitly assign an ACL to. Conversely, each ACL can be assigned to many Technical Data Resources, hence providing re-usability of each ACL, and again making administration of access controls easier.

The example illustrated here is one of many access control configurations that are possible with the digital engineering environments and TDMS's available today. The design and implementation of a robust access control scheme is essential to successful Technical Data Management. As such, it should be treated as a system-engineering project unto itself, using the tools and techniques an SE would employ on any project of any complexity.

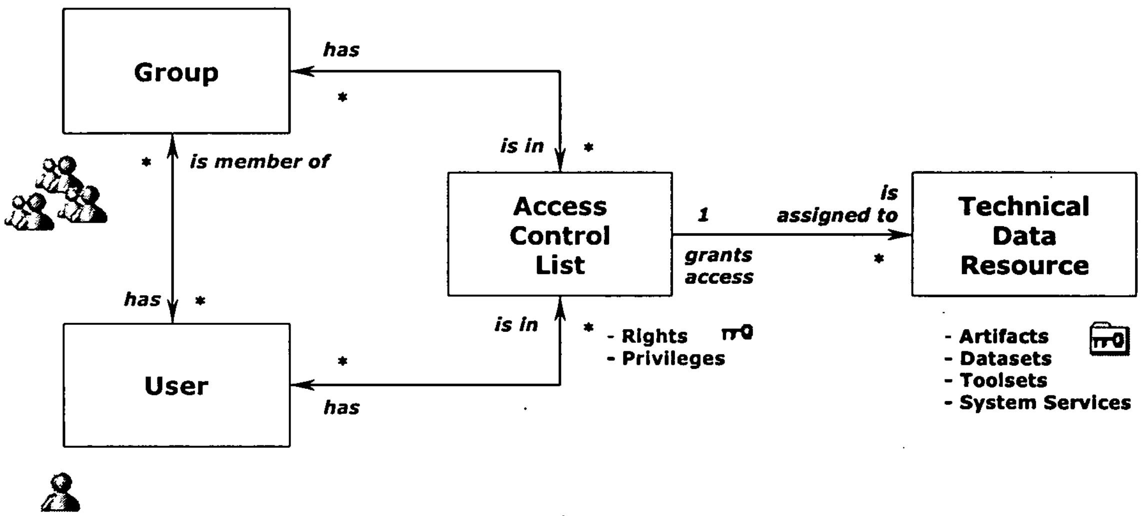

Figure 17.3.5-1. Access controls can be based on any number of control models. In this example, Access Control Lists (ACLs) associate specific users – either individually or via groups - to Technical Data Resources (artifacts, datasets, tools, etc.), along with the rights and privileges they have to the resource.

17.3.6 Maintain stored technical data in a manner that protects it against foreseeable hazards such as fire, flood, earthquake

A TDMS represents an investment typically measured in millions of dollars by an organization, and is the backbone of the digital engineering environment the organization depends on daily. Successfully implementation and operations can quickly turn to failure in the face of events such as fire, flood, hurricane, earthquake, riots or other destructive acts. Preparation is key to dealing with events such as these.

A Disaster Recovery and Continuity of Operations Plan (DRCOP) prepares the organization to deal with potential disasters. It also provides the basis for dealing with routine occurrences such as the accidental deletion of a working file by an engineer, or the unintentional deletion of a folder structure holding released drawings by an CM administrator. Mistakes occur; being ready is the key.

A DRCOP is very simple in principle; it first assumes that a destructive event has occurred (whether foreseen or unforeseen) and second, it outlines processes and procedures that must be followed to maintain continuity of business operations and to recover the system back to an operational state. The key aspect is that processes and procedures must be in place *before a destructive event occurs*! Once a disaster occurs it's too late to begin thinking about backing up the system or working on alternate or failover operating sites. The focus of a successful DRCOP must be ***proactive***.

The SE establishing the TDM process for an engineering organization will rarely be solely responsible for a DRCOP. Planning for disaster recovery is a collaborate effort spanning the Information Technology infrastructure provider, the system operator, and possibly other organizations. The participants involved depend on the acquisition strategy the organization or agency employs to host the TDMS. The SE plays a key role in providing inputs regarding the TDMS service levels that are necessary to support the organization's engineering processes, as well as the cost impacts of the system being unavailable under various scenarios. The cost impacts are used to determine the most effective backup and recovery strategy for the organization.

The elements of a sound DRCOP must reflect the platform and system architecture of the TDMS. It must also reflect a balanced approach to the tradeoff between risk mitigation costs and benefits. If not, it will falter under the burdensome cost of implementation. To be effective, a DRCOP must be tested and validated on a periodic basis. Just as a smoke detector with dead batteries gives a false sense of security, an elegant and detailed DRCOP that is untested gives the same false sense of security.

Some elements that form the core of a robust DRCOP are:

- Data and Content Backups – Backups provide the fallback position you move to when all else fails to resolve a problem or recover the system. Backups can also be used on an ongoing basis to recover specific files or folders that must be restored due to routine actions – accidental deletion, corruption, etc.

- Backup Frequency and Schedule - The frequency of backups and the schedule they run on will be dictated by operational constraints (when does the system have to be available to support users, when does system maintenance have to be performed), the performance and configuration of the backup system (backup speed, whether verification of backup media is included, etc.) and the size of the system at any point in time (size determines how long the backups will run – all other factors being equal).

- Backup Media Storage and Retrieval – Storing backup media is a key decision in the DRCOP. Storing it in the same location as the system itself puts it at risk under certain disaster scenarios (hurricane, earthquake, fire, act of terrorism, etc.). Storing it at an offsite remote location is a prudent step. The distance of the storage location from the system itself and the means to access the backup media are factors in the timeliness to restore the system from backups.

- Hot Standby and Fail Over – If the TDMS is critical to the mission of the enterprise, say for financial (e.g. revenue generation) reasons or safety reasons, unavailability to recover from backups may not be acceptable. In cases such as these, the DRCOP can specify the installation and use of hot standby hardware or establishment of fail over sites that replicate the system infrastructure and provide the means to continue operations on very short notice. The timeliness of the switch to hot standby hardware or fail over sites is driven by the architecture of the TDMS and the design of the alternate support elements. In most cases, hot standby and fail over will significantly increase the cost of implementing and operating the TDMS. Cost-benefit analysis and return on investment analysis is a key aspect of determining how aggressively these techniques are employed in a DRCOP.

- Content and Data Recovery Procedures – Having backups in place and hot standby or fail over sites ready to step in is meaningless if procedures to use these elements to continue operations or to recovery the system do not exist. Recovery procedures are one of the most important aspects of a sound DRCOP. The procedures should be detailed enough to outline on a step by step basis the processes involved in failing the system over, or recovering part or all of the system. A best practice is procedures that segregate the steps by role and provides an integration process that coordinates actions among the various roles.

- Content and Data Recovery Test Scripts – Any recovery procedure that is used for the first time when actually needed involves extreme risk. The best-laid plans are often tripped up by the unexpected. The solution is to develop test scripts that exercise recovery procedures before they are actually needed. This also server to train system operators and support staff on recovering the system, building their proficiency in executing the procedures and minimizing the time needed to recover the system.

17.3.7 Backup and archive artifacts for recovery and future uses

The backup of data and content for system recovery purposes – whether caused by accidental human error, system failure, or disaster – is covered by the DRCOP as explained in the previous section (17.3.6). An archive, on the other hand, is a set of records that have been created during the SE lifecycle and have been specifically set aside for long-term preservation. The "backup" of data and content for archival purposes requires processes and procedures that are distinct from the backup of data and content for system recovery purposes. The distinctions lay in three main areas:

- The format the archived record assumes; typically a format that is long-lived with respect to the technology that created it and the technology used to access it.
- The location of the archived records; typically an independent repository dedicated to archival purposes and setup for long term reliability with respect to the data storage media involved.

- The procedures used to access archived records; typically involving a librarian department, organization or function tasked with creating and maintaining the archive.

Archival requirements need to be explicitly addressed as part of processes or procedures dedicated to this function, and capabilities within the digital engineering environment or TDMS must be provided or configured to support archiving. Archival requirements are driven from several perspectives, including the goals and objectives of the organization, by specific archival requirements within contract Terms and Conditions, by government or industry regulations (for example U.S. Government Code of Federal Regulations (CFR) Title 36 Part 1234.30 - Standards for the Creation, Use, Preservation, and Disposition of Electronic Records), and by records retention policies that reflect the legal and risk mitigation stance of the organization.

Cost-benefit analysis often comes into play into the implementation of archives since the usefulness of a project's history and artifacts in the future must be balanced against the cost to create and maintain the archive. Practical paybacks in areas that are rapidly changing with respect to the base of knowledge involved are unlikely. In these cases, archives must be are justified more along the lines of historical preservation rather than any reuse of archived records in future projects.

17.4 Provide Technical Data to Authorized Parties

The overall goal of TDM is to capture, manage, and provide technical data to authorized parties in a timely and effective manner. The essence of the systems and toolsets that support it is the maintenance a library of engineering artifacts, content and reference data that are relevant to user needs. Strong user interfaces to quickly and conveniently find, retrieve and use the information are critical to its success.

17.4.1 Maintain information library or reference index to provide data available and access instructions

The TDMS and digital engineering environment of a large organization will house enormous volumes of data and content. Tens of millions of data objects covering many terabytes of disk space is not uncommon. Even mid-size organizations will have repositories that hold thousands of drawings, documents and models. The challenge this vast amount of data and content poses is to be able to find what a user is looking for quickly and effectively.

Fortunately, the SE building a TDM process has a broad array of tools and techniques available that can be plugged into the TDM infrastructure to host data delivery user interfaces based on popular web search engines such as Google, or to build portals tailored to the data and content needs of the SE life cycle. Toolsets such as Business Intelligence (BI) systems, Data Mining (DM) systems, Data Warehouses, Decision Support Systems (DSS), and Knowledge Management (KM) systems are available to augment basic search and retrieval capabilities for the data and content housed in the TDMS.

Tools that are awkward to use, assume unlikely user knowledge or behavior, or provide inadequate or inaccurate results are fatal. It is essential that usability of search and retrieval tools be at the forefront of the TDM data delivery strategy.

Figure 17.4.1-1 illustrates an SE portal that provides an index to engineering process documentation. This is organized along the lines of the SSE process hierarchy presented in Figure 17.1-1. Each process area is color coded and broken down into its sub processes. Next, process specifications in the form of Internal Operating Procedures (IOPs) are listed, as well as the templates and forms that the IOPs callout to execute the engineering lifecycle.

Each IOP, Template and Form callout is a hyperlink that brings up the specific item form the TDMS when clicked. The leftmost column contains a set of hyperlinks to resources that the SE would typically need in the course of a project. Links to other portals, document trees, artifact tress, and templates provide convenient access to the engineering content that an SE would need when working an assignment. Links to computer-based training and digital engineering environment tools are provided, as well as links to other websites and web-based tools that help the SE perform their job in a more effective manner.

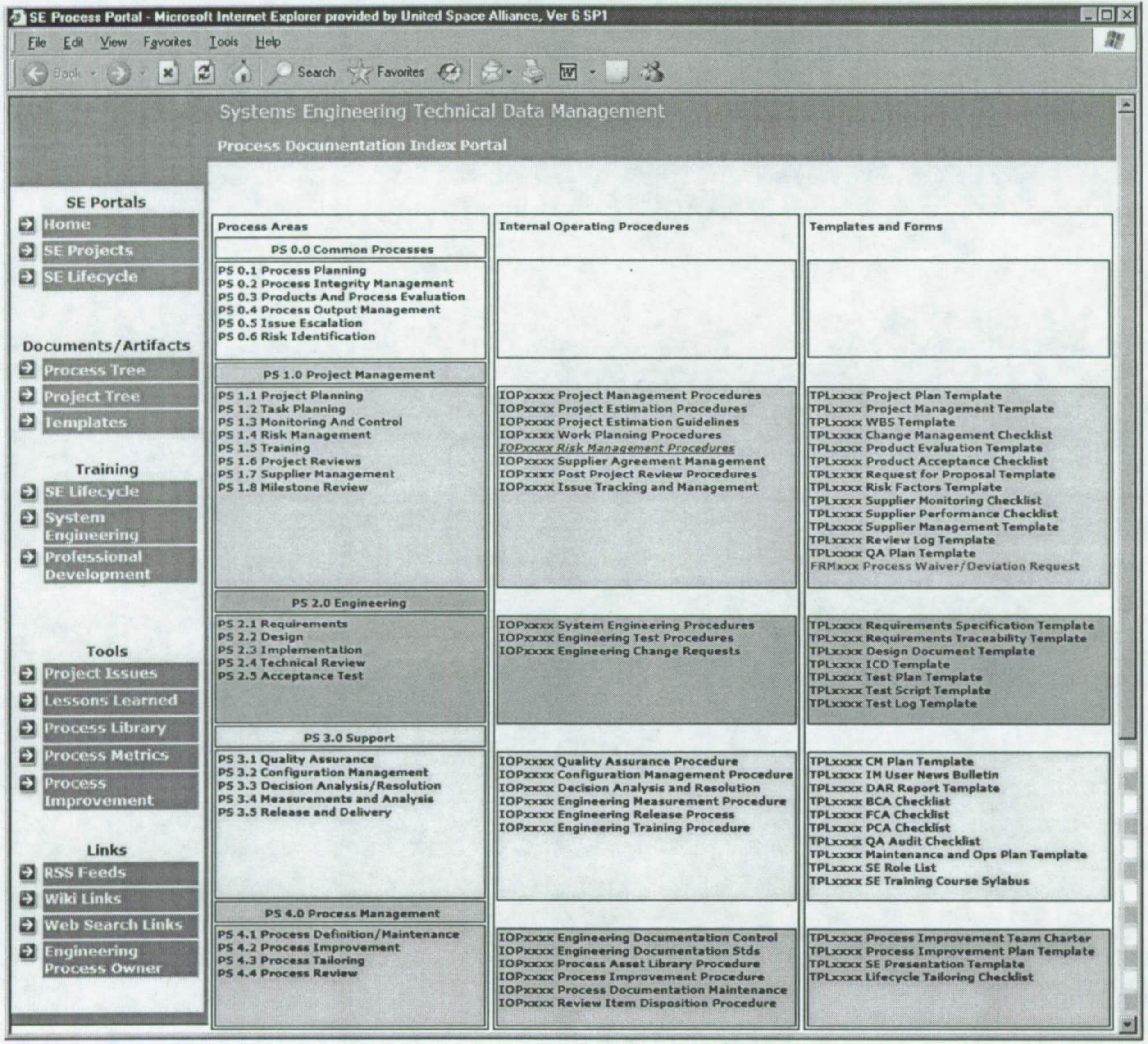

Figure 17.4.1-1. A web-based portal provides the SE with a reference index to Engineering Processes, the associated Internal Operating Procedures and the Templates and Forms needed to execute the SE lifecycle. Each procedure, template and form callout is a hyperlinks that brings up the specific item. A series of hyperlinks in the leftmost column provides easy access to other SE portals, documents, artifacts, online training, tools and engineering related web sites.

17.4.2 Receive and evaluate requests for technical data and delivery instructions

Receiving and evaluating requests is simplified if some form of automated user registration system is employed to administer user accounts and user access levels across the numerous tools and data sets that comprise the digital engineering environment and TDMS. In addition to providing users with a single focal point for requesting and updating access, a registration system provides the organization with a consolidated view of who has access to what, and provides a framework to implement control procedures such as account approval workflows, periodic revalidation of system access, and license management in cases where access requires licensed commercial off the shelf (COTS) software.

An automated registration system also provides the framework to establish access rights, limitations, obligations, and commitments with the user via agreements they enter into during the access or account registration process. This may be essential in certain government settings, and useful in other settings.

Today, the SE or IT organization that is setting up an automated registration process has many COTS tools to choose from under the Identity Management (IdM) umbrella. IdM covers many facets within the access control arena, including user account management, password management, policy and role based access management, and directory services, among others. Creating user accounts when needed and inactivating them when appropriate is referred to as provisioning and de-provisioning. IdM tool suites typically provide workflows to handle user account and user access provisioning, as well as workflows or triggers to de-provision (inactivate) accounts and access under the range of business scenarios that drive this functionality.

Figures 17.4.2-1 through 17.4.2-3 show a hypothetical user interface for requesting access to the variety of managed systems that would comprise a typical digital engineering environment and TDMS. The process begins by identifying a person who is requesting an account or access to be setup. If the person does not have an existing account (i.e. a new user), they are prompted to enter information that uniquely identifies them. The information required would be driven by the business polices and practices of the organization involved. If the person has an existing account (e.g. a current user requesting access to an additional system), the identify information would be retrieved from the system and displayed for the requestor to confirm.

The process continues by prompting the requestor for the application (for system access) or facility (for new user accounts) they are requesting access to. Justification for the request, the type of role they will perform, groups they need to be in, or the profile they will need might also be requested.

The request submittal ends with the requestor validating the data they entered and acknowledging their responsibilities under the policies and procedures of the organization. Pressing the "submit" button is electronic acceptance of their responsibilities. If a more formal and rigorous electronic signature is required, the user interface could be modified to include an electronic signature handler that would provide this feature.

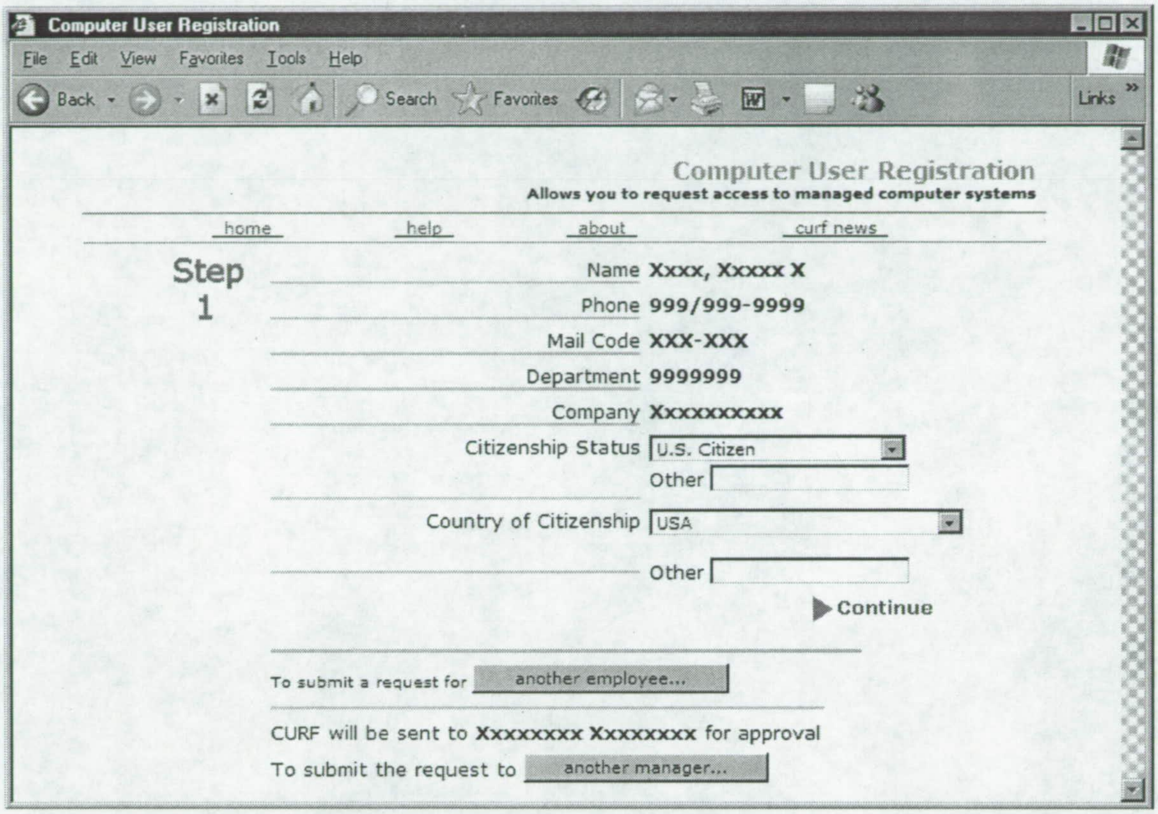

Figure 17.4.2-1. An automated user /access registration workflow begins by identifying a new or existing user. Attribute data that uniquely identifies a person is captured or displayed. This information would be already be filled in by the IdM system for users with existing accounts.

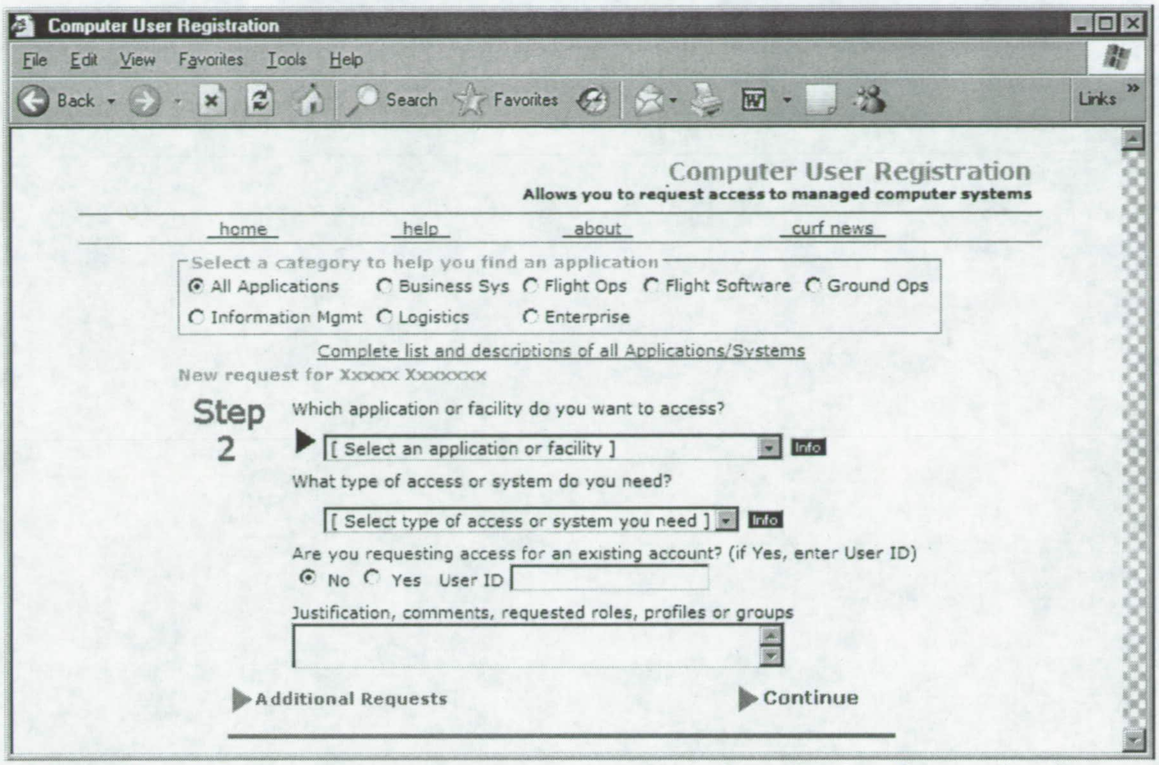

Figure 17.4.2-2. The registration process continues by selecting the application or facility involved, and providing information on roles, profiles, groups and justification.

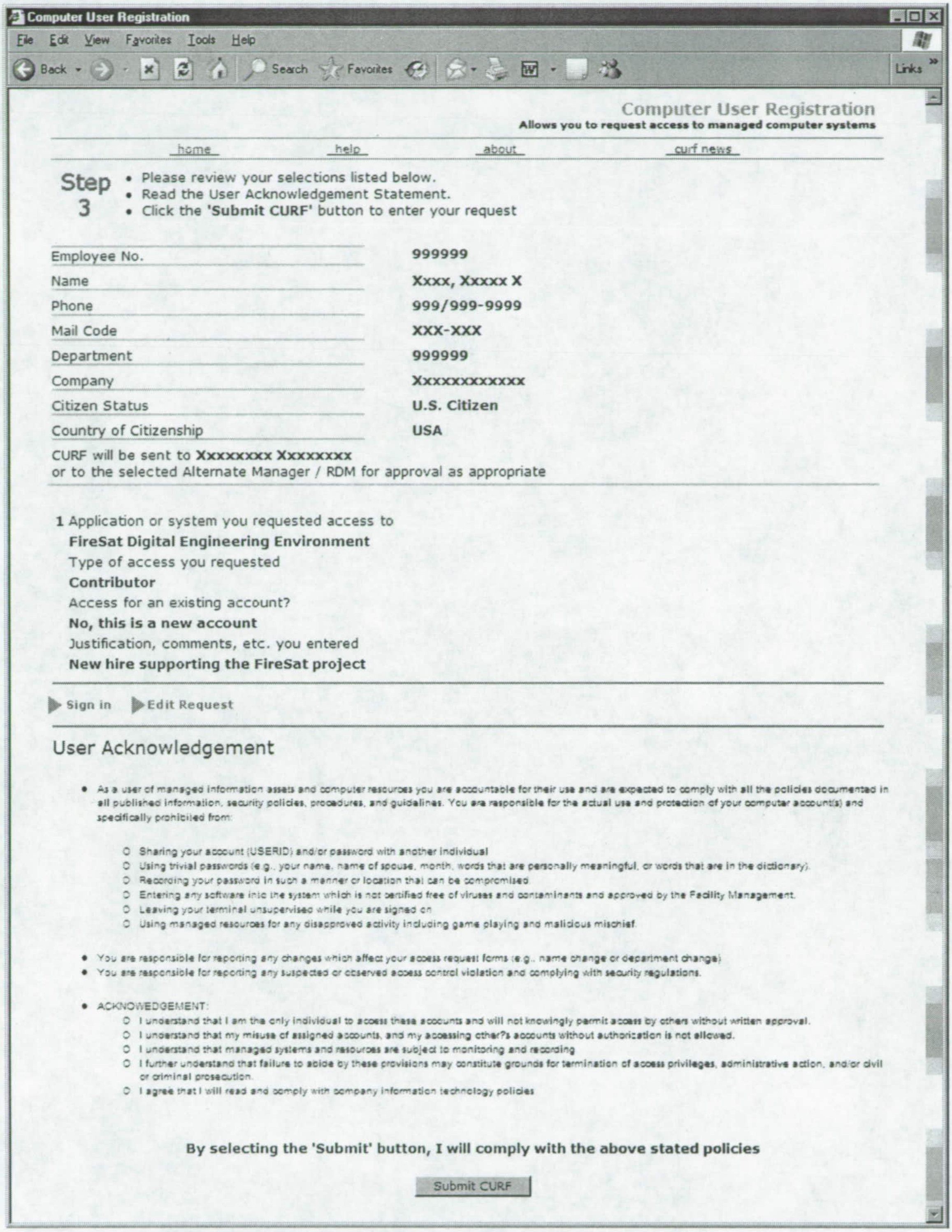

Figure 17.4.2-3. The request is submitted for processing. The submittal provides electronic acknowledgement of the requestor's understanding of the policies and procedures they must comply with.

Submitting the request could kick off a workflow that routes the request for approval and implementation. Typical steps may include approval by a sponsor or agent, approval by a Data Owner who is responsible for stewardship of the data and content that access is requested for, and processing by a System Administrator or automated routine to setup the user's account, permissions and rights. The request process must provide feedback to the requestor and other parties involved in the approval workflow as the request proceeds, as well as transmittal of account and access credentials to the requestor in a secure fashion when the request is approved (or the reason for rejection when a request is not approved).

17.4.3 Confirm that required and requested technical data is appropriately distributed to satisfy the needs of the requesting party and in accordance with established procedures, directives, and agreements

Sound account management policies include periodic revalidation of user accounts and access rights. Revalidation on an annual or semi-annual basis is typical, and involves routing approved requests to the sponsors and Data Owners for review and recertification of each active account. An automated account management process should be designed to provide features that make account revalidation quick and efficient. Features that make revalidation quick and efficient include:

- Online list of active accounts due for revalidation, filtered by approval role
- Ability to filter accounts due for revalidation by specified criteria
- Ability to display account information, history, permissions and rights
- Ability to re-approve or disapprove an individual account, a selected list of accounts, or a block of accounts
- Automated notification of account disapproval (to sponsors and users)
- Automated deactivation of accounts that are disapproved, either by explicit disapproval or via expiration (i.e. an account is not re-certified within a specified grace period from the re-certification date)

Figure 17.4.3-1 shows a web-based re-validation page that allows system managers to review active accounts that are due for revalidation, and approve or disapprove their continued use. This page displays the access requests approved by the manager performing the revalidation, and allows them to easily update each account with their disposition. Click on the blue "Info" icon next to a request will open a window with the details for that request. Approving an account for continued use updates the account's attribute data that typecasts it as either active or inactive, and resets its annual verification timer.

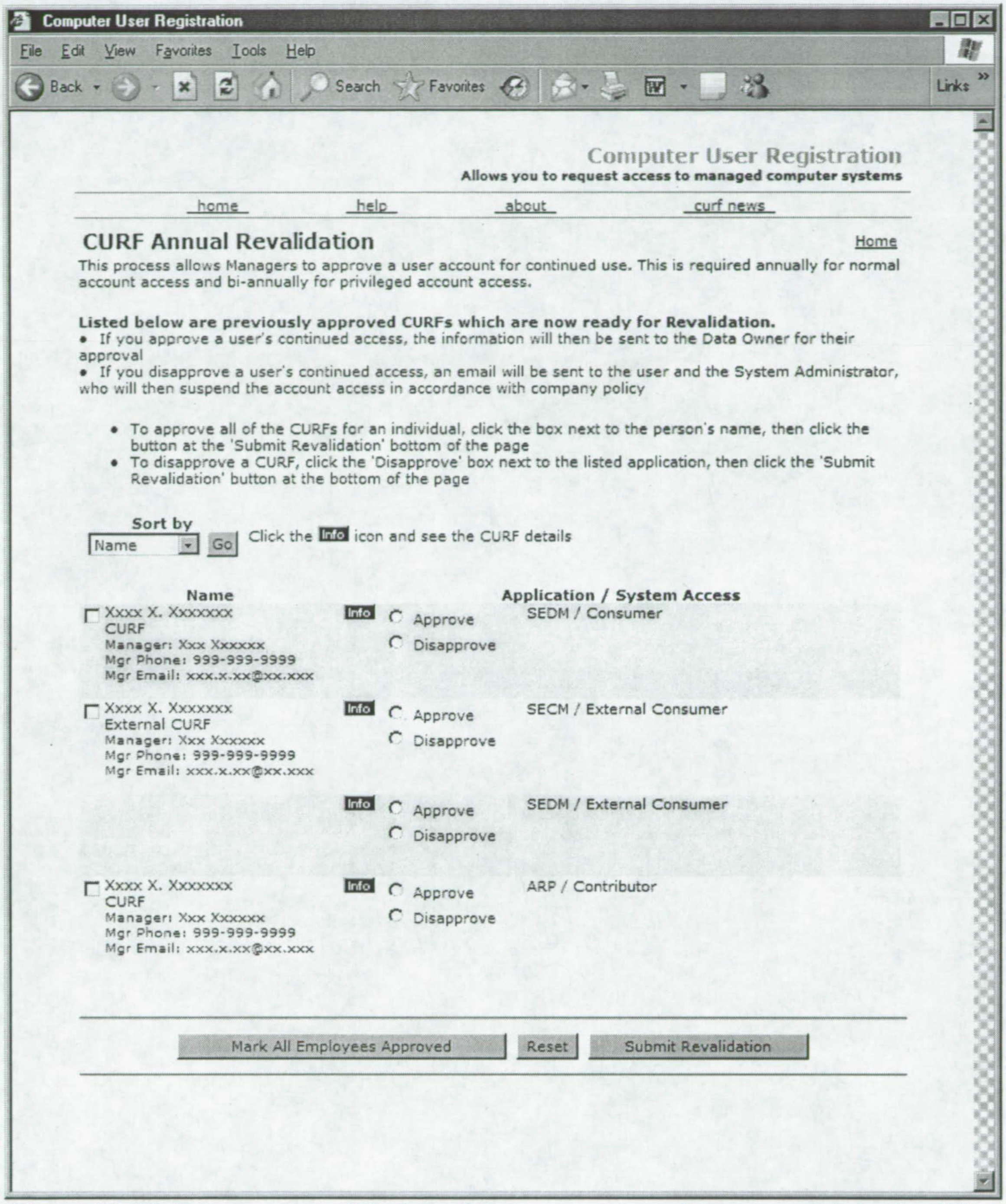

Figure 17.4.3-1. Annual revalidation of user accounts and access grants is simplified by providing an automated user interface for this purpose. This is essential when thousand of accounts and access grants must be revalidated on a periodic basis.

In certain situations such as an employee being terminated for cause, an accident investigation, or a student being expelled, for instance, it may be necessary to remove access to the digital engineering environment and TDMS immediately. User account management procedures should address this situation if required, and provide the criteria, contacts and processes to do so.

17.4.4 Confirm that electronic access rules are followed before allowing access to the database and before any data is electronically released or transferred to the requester

The design and configuration of the access controls outlined in chapter 17.3.5 and the access request and approval processes outlined in chapters 17.4.2 and 17.4.3 must work together to ensure access to engineering artifacts and data complies with the data governance policies and rules of the organization. The mechanics of granting access typically involves adding approved users to the appropriate groups, roles, or other control structures provided by the access model employed by the TDMS. Once established, ongoing maintenance of user accounts, and the groups, roles or access rules they are participating in, is necessary as personnel come and go or circumstances change (promotions, role changes, leaves of absences, etc.).

17.4.5 Provide proof of correctness, reliability, and security of technical data provided to internal and external recipients

Audits are used to provide proof that established procedures, directives, and agreements are being followed. An audit of the SE digital engineering environment and TDMS will evaluate the systems and processes that makes it up, and will sample content and data it manages from projects or products it was employed for.

In most large organizations, an internal audit group is responsible for performing audits. The auditors will focus on business processes to ensure compliance with external and internal standards and procedures, and generally accepted practices. Additionally they will evaluate the supporting systems and toolsets to ensure the correctness and reliability of the artifacts produces under the processes and procedures in place. In situations where internal audit groups do not exist, external auditors can be contracted to conduct the audit and certify the results.

An audit of the SE lifecycle and associated TDMS will focus on evaluating SE practices, procedures, and systems to confirm that required and requested technical data is appropriately captured, managed, and distributed to satisfy the needs of the project teams and their customers and that lifecycles are being executed in accordance with established procedures, directives and agreements. An audit will:

- Review content and data submissions against TDMS quality controls and standards to evaluate the accuracy and integrity of content and data, and gauge the effectiveness of the input edit checks and validation features.

- Review exception-handling processes to gauge the effectiveness of exception detection and resolution.

- Review data backups and DRCOP recovery procedures, and review the results of periodic DRCOP testing.

- Review users accounts and evaluate the effectiveness of user account management procedures; random samples of CURF approvals and implementation provide a gauge of the effectiveness of account provisioning and de-provisioning processes.

- Review access controls and mechanisms; random samples of access controls provide a gauge of the effectiveness of access control processes.

- Review all privileged user accounts; evaluate rationale and necessity

- Document all audit results and findings

- Track finding through resolution and re-test

An audit provides proof of correctness, reliability, and security of the data and content stored and managed within the TDMS. It provides a level of confidence to internal and external users and stakeholders of the services and functionality delivered by the TDMS.

17.5 Collaborate through Effective Use of System and Process Artifacts

System Engineering is rarely an individual effort. Integrated Product Teams (IPTs) and other forms of teaming are the norm. These project structures bring together the skills and expertise from the multiple disciplines that are necessary to engineer the complex systems that are prevalent in our digitally driven world. Modern digital engineering environments and their underlying data architectures (see Figure 17.1.4-1) provide the key infrastructure that enables these teams to be successful. Electronic collaboration environments and Integrated Data Management (IDM) systems often augment digital engineering environments and their TDMS's to support engineering project teams, whether they are composed physically, functionally, or along other lines.

Collaboration tools and environments range from widely available standalone tools such as email and distributed file shares, all the way to highly specialized COTS packages designed and marketed specifically for collaboration. High-end packages typically provide an integrated set of tools using familiar paradigms such as electronic rooms, shared cabinets and folders, or virtual spaces, and are up-and-running when the installation process completes. Low-end collaboration environments are typically composed from standalone components or tools (for example, email services and file shares), and place the burden of integrating individual tools on the organization or enterprise assembling the collaboration environment.

17.5.1 Use collaboration tools and techniques

Effective collaboration requires tools and techniques to communicate both synchronously (e.g. phone call, Internet chat, instant messaging, etc.) and asynchronously (e.g. voice mail, email, fax, etc.), and tools and techniques to interact as a collective group (e.g. audio-video conferencing, virtual whiteboards, teleconferences, etc.) or as subgroups (wiki's, blogs, Internet forums, etc.). In addition, coordination of group, subgroup and individual efforts requires the use of management tools and techniques, including scheduling systems, shared calendars, task, action and issue management tools, workflows, and content lifecycles, among others.

As the web evolves into second-generation capabilities, its tools, techniques and underpinnings also become candidates to assist in the collaboration needed to bring team-based SE projects to successful conclusion. For example, social networking sites focus on the development of online communities linked through pre-defined interests or themes or through user-defined interests or themes. The tools and techniques employed in these arenas for user interaction, group formulation, and information sharing evolve rapidly and provide opportunities for application within the SE collaboration arena.

17.5.2 Use search and retrieval tools and techniques

The overall goal of the TDM process is to capture and manage the digital artifacts associated with the SSE life cycle, and to provide this data and content to authorized parties. The heart of the data delivery capability is a strong user interface to search, retrieve, and use SSE generated information. Search and retrieval tools are central to the user's experience, and thus determine the effectiveness of the system

Figures 17.5.2-1 and 17.5.2-2 illustrate a web-browser based search and retrieval portal tailored to policies and procedures defining the SE life cycle. The portal consists of a selection page that enables the user to select various catalogs to search against (e.g. Contract Specific documents, Company Policies, Operating Procedures, etc.) and set specific search criteria (e.g. Document Number, Document Title, Status, etc.). The selection page also allows the user to search within the content of the documents by specifying words to search for. FireSAT could use a portal such as this one used in NASA's Space Shuttle Program.

Once the user has set search location(s) and specified search criteria, they submit the search for execution. The TDMS is searched, and the results are presented to the user. The results page displays the search criteria entered by the user, as well as the documents that matched the criteria. Summary information for each hit is displayed in grid fashion (Document number, title, revision, etc.), and includes an information icon displayed as a white "i" in a blue dot. Clicking on the document number hyperlink with display the document for viewing. Clicking on the information icon will open a details page that presents all the attribute information for the specific document in question. The user can select the number of items to return per page, and can scroll through the results page or user the browser find feature to search for terms within the results page.

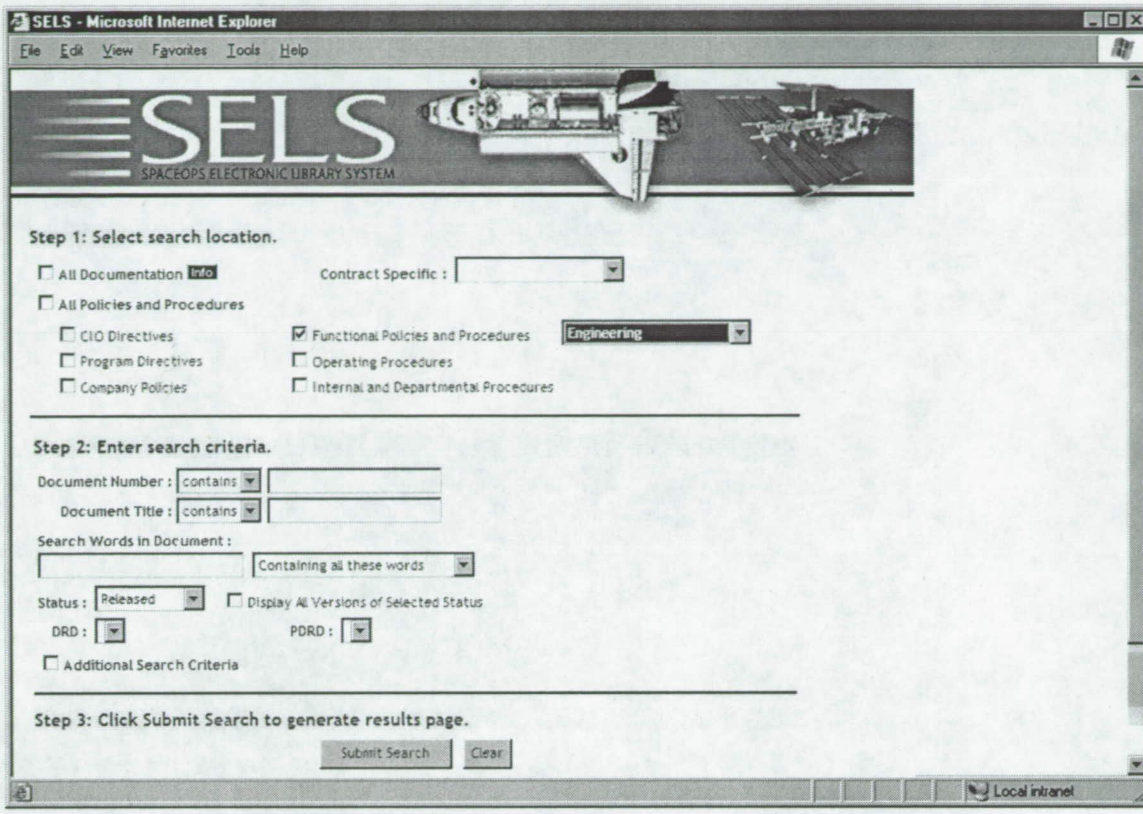

Figure 17.5.2-1. System Engineering Search and Retrieval Portal. This portal supports searching multiple locations within the TDMS repository based on search criteria set by the user.

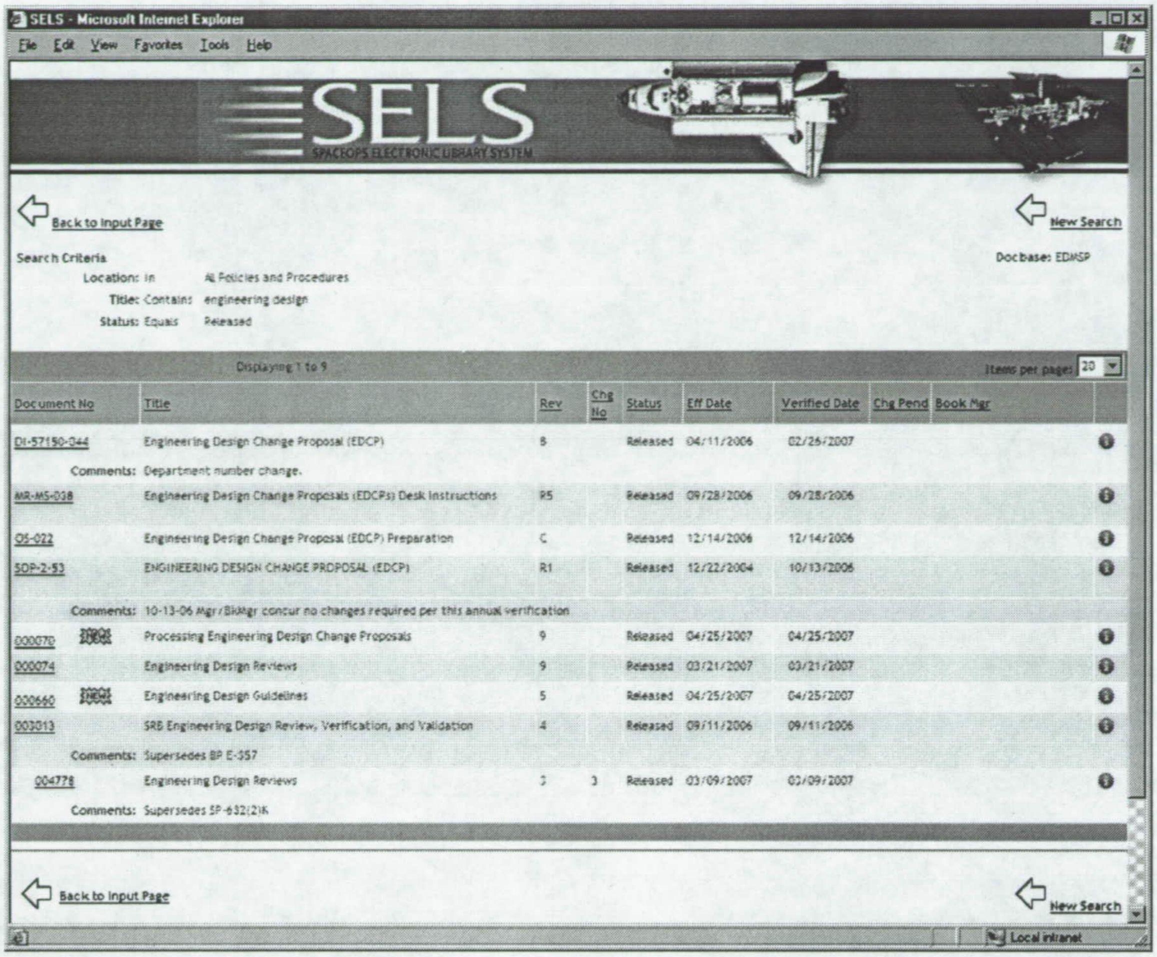

Figure 17.5.2-2. System Engineering Search Results Page. This page displays all the documents within the TDMS repository that match the search criteria set by the user. The document can be displayed by clicking on the document number hyperlink, or detailed information about the document can be displayed by clicking on the info icon at the far right in each results row.

In many cases the project team developing a product or system is composed of personnel from multiple disciplines. Each discipline brings a different skill set, vocabulary, vernacular and perspective on the SE lifecycle and the artifacts involved. This makes search and retrieval of artifacts challenging when traditional search by attribute or search by keyword is used. In many cases the same item or concept is referred to differently across skill and expertise boundaries, hence placing a burden on the user to understand the differences and reflect them in their searching.

Figures 17.5.2-3 through 17.5.2.8 illustrate a solution to this challenge. In this case, the search and retrieval application is setup to enable users to establish a visual context for searching by drilling down into illustrations of hardware or topical baselines. Within the visual context, users can also set search filters applicable to the context using a dashboard that is visible for this purpose. Users can retrieve results sets by clicking on any results hot spot within the drilldown. Using a visual search and retrieval approach removes the burden of understanding nomenclature and identifiers from the user and places them on the system, which creates fully qualified queries in the background, based on the visual context and filters established by the user.

Figure 17.5.2-3. An Integrated Data Management (IDM) web site based on visual search and retrieval techniques. This portal supports searching various different data and content domains by establishing a visual context and setting filters to narrow the results returned by the search.

Figure 17.5.2-3 shows the home page of the Attentus Integrated Data Management web site. The links on the left side of the page show the data and content domains this instance of the application is configured to support; in this case, various NASA Human Space Flight programs. Each domain callout is a hyperlink to collections of data and content baselines associated with the topic.

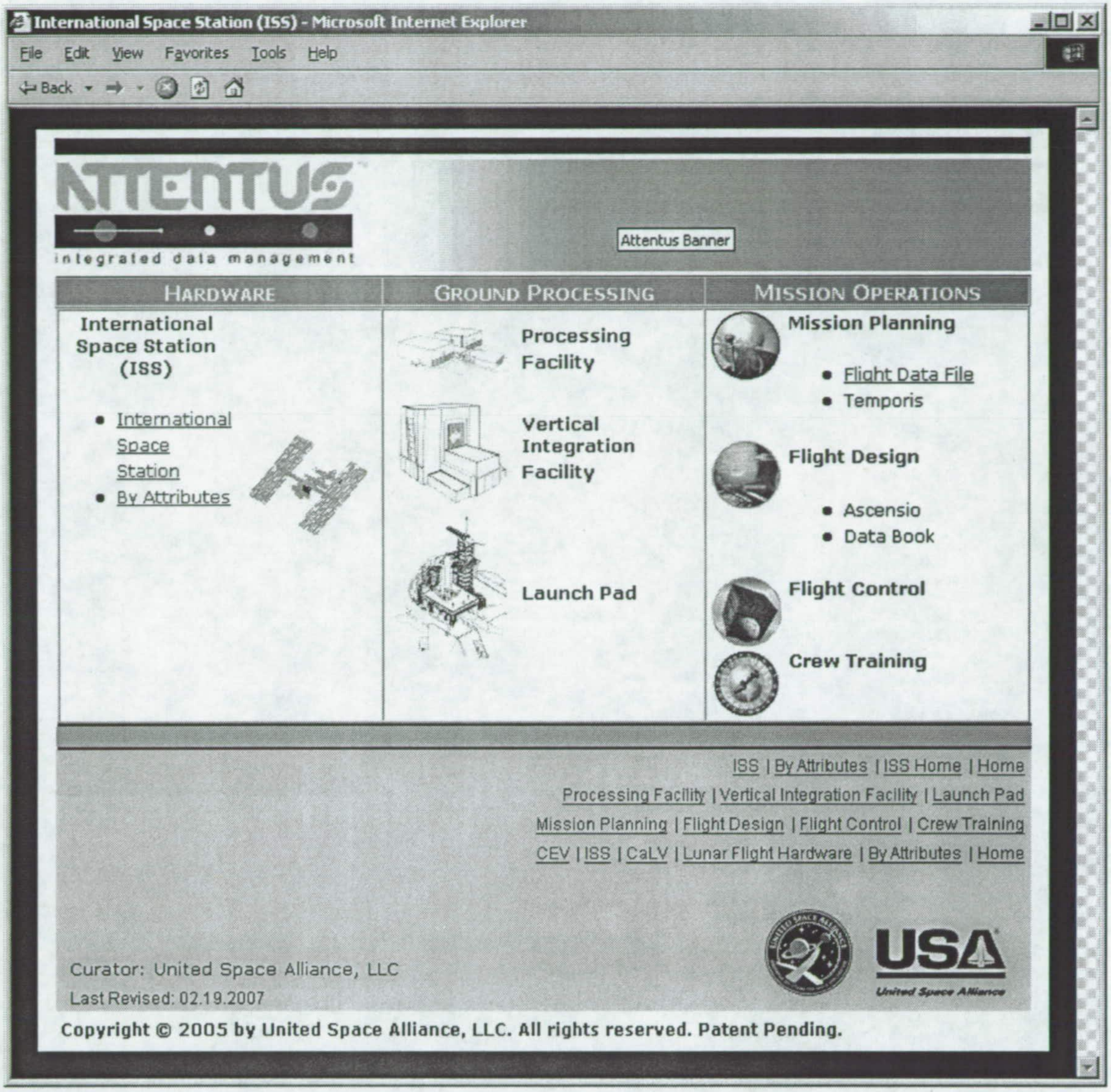

Figure 17.5.2-4. This IDM portal is configured to search collections of baselines associated with ISS Hardware, Ground Processing facilities, and Mission Operations topics. Each baseline can be drilled into via hyperlink or hotspots located on the web page.

Figure 17.5.2-4 shows three data and content collections, one for Hardware, one for Ground Processing facilities and one for Mission Operations. Each collection is made up of one or more data and content baselines. Each baseline would typically contain the SE lifecycle artifacts associated with its engineering, and any other data or content the organization chooses to store in the TDMS associated with that baseline. Accessing the baselined data is through the hyperlinked baseline titles or through hotspots on the illustrations associated a baseline.

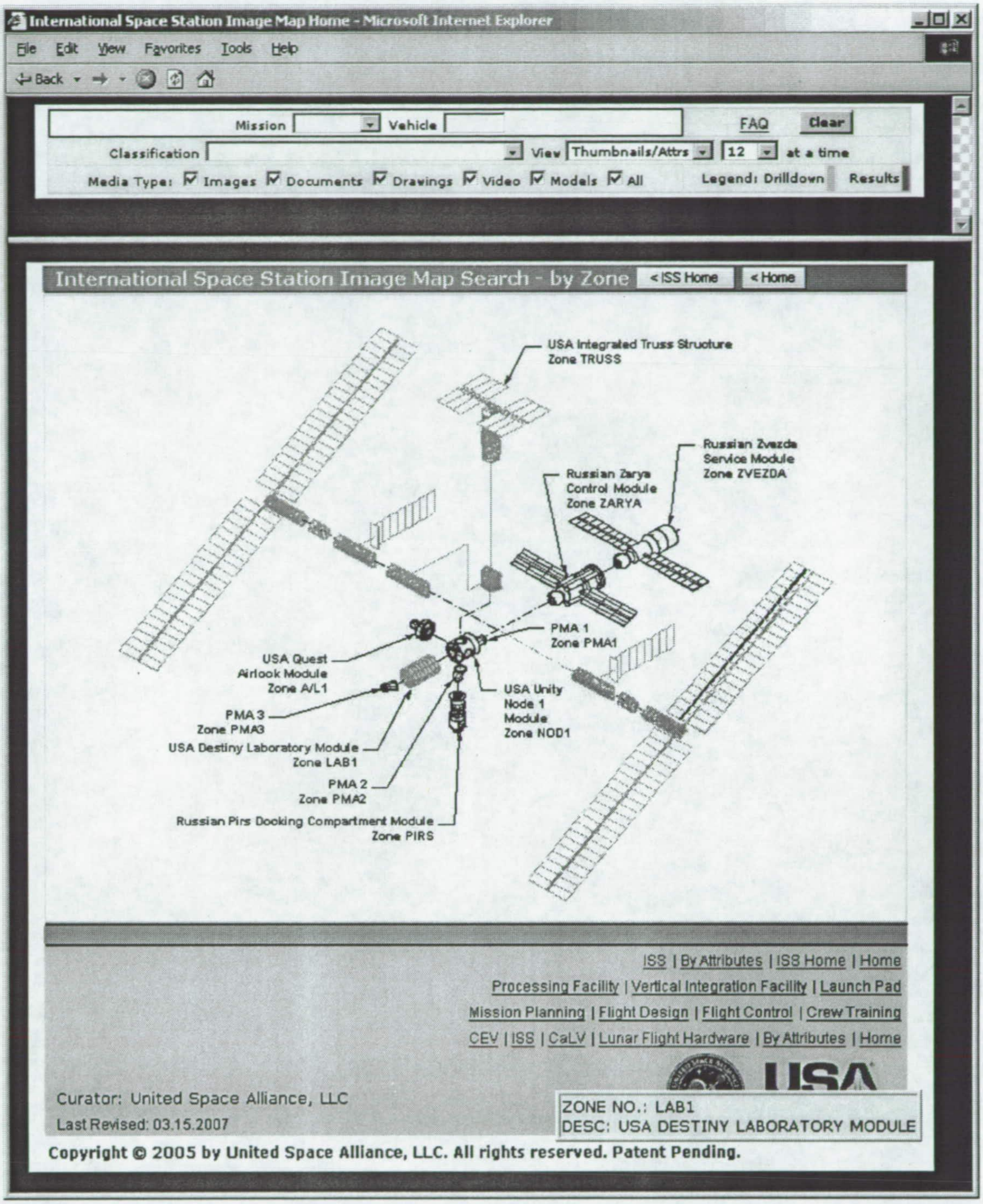

Figure 17.5.2-5. The ISS hardware baseline enables the user to drilldown into any of the modules or assemblies that are on-orbit or being processed for launch.

Figure 17.5.2-5 shows the top level of a baseline, in this case the International Space Station (ISS). Each baseline is sub-divided into logical "zones" based on a physical or topical breakdown. Each zone is a hotspot is that highlights as either blue or yellow when a pointing device (typically a computer mouse) hovers over it. Yellow indicates further drilldowns are available, while blue indicates the lowest level of drilldown has been reached and search results will be returned if the hotspot is selected. The dashboard at the top of the page allows users to set search filters that are integrated with the drilldown to narrow the set of results returned. The information box in the lower right corner pops up as the user moves their pointer over the various zones, providing information about each hotspot.

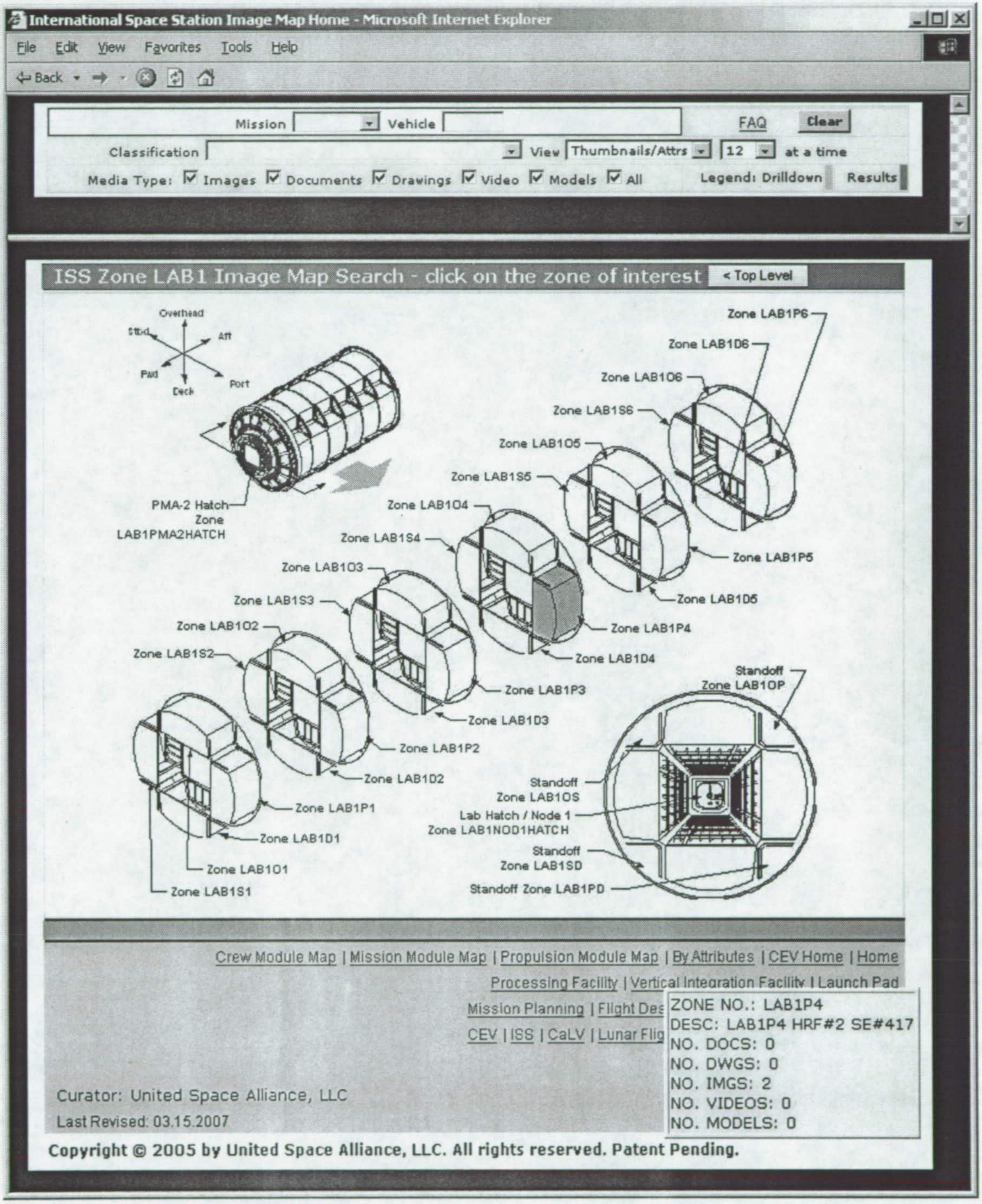

Figure 17.5.2-6. The ISS lab drilldown presents users with multiple results hotspots. Positioning the mouse or pointer over a results hotspot displays its color in blue and pops up an info box in the lower right corner that summarizes the content that will be returned based on this visual context and the search filter the user has set via the dashboard.

Figure 17.5.2-6 shows a drilldown at the lowest level that returns results. The info popup in this case summarizes the data and content by type that will be returned if the user selects this hotspot. This is based on the zone selected and the filters set in the dashboard. In this manner the user gets real time feedback on results without having to actually execute the query.

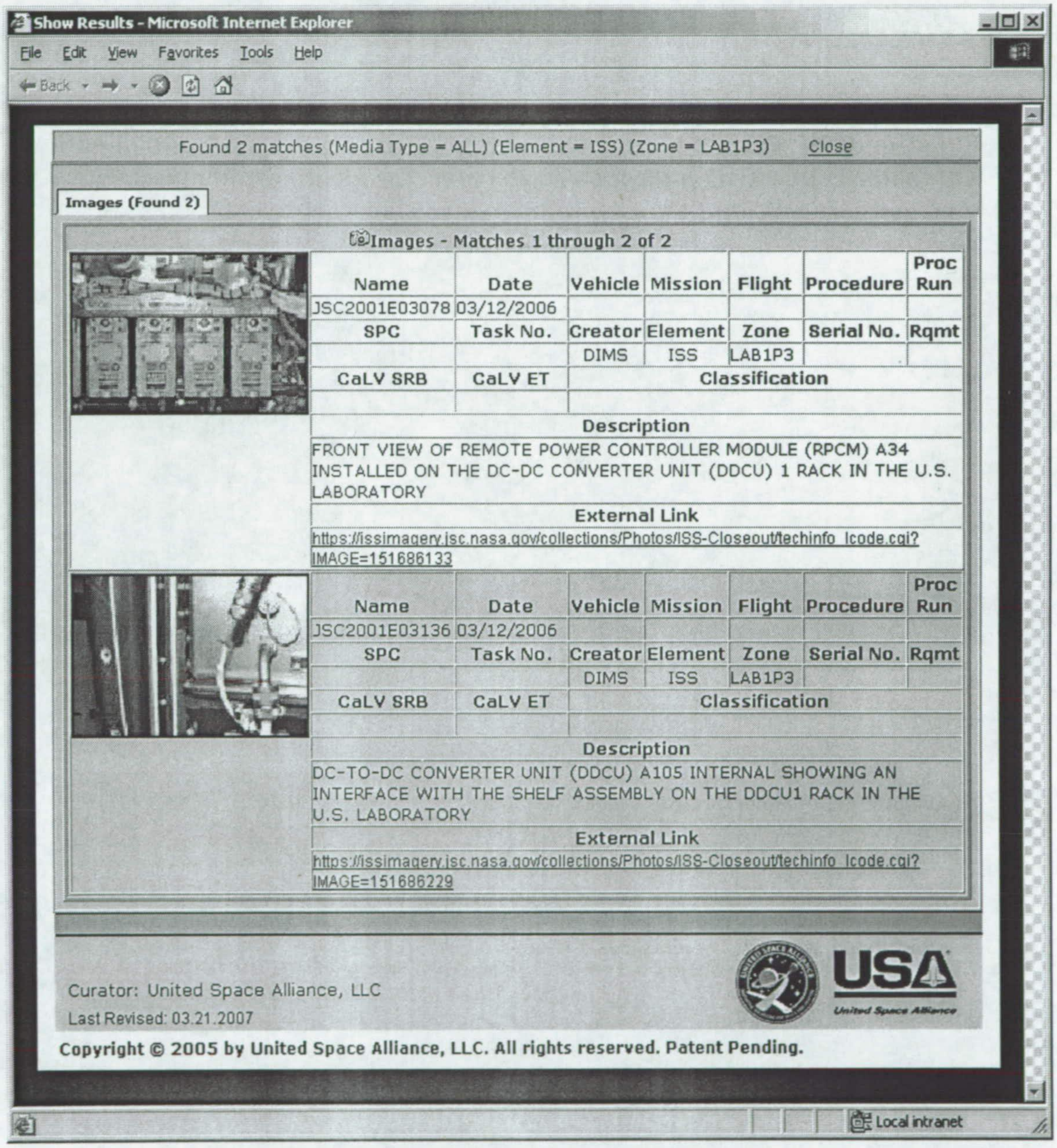

Figure 17.5.2-7. Search results are presented in grid fashion along with the data attributes stored in the system that describe each item. The thumbnail of the item enables the viewer associated with the content to be launched.

Figure 17.5.2-7 shows the results returned by a query. Each piece of data or content returned is displayed in thumbnail form, along with the data attributes the system stores for it. The display of information is controlled by selections on the dashboard. The type of thumbnail presented (icon, miniature, etc.) depends on the content type. Clicking on the thumbnail launches the appropriate viewer to display each piece of content. If the content is stored in an external repository, it can also be accessed via an external hyperlink stored for this purpose.

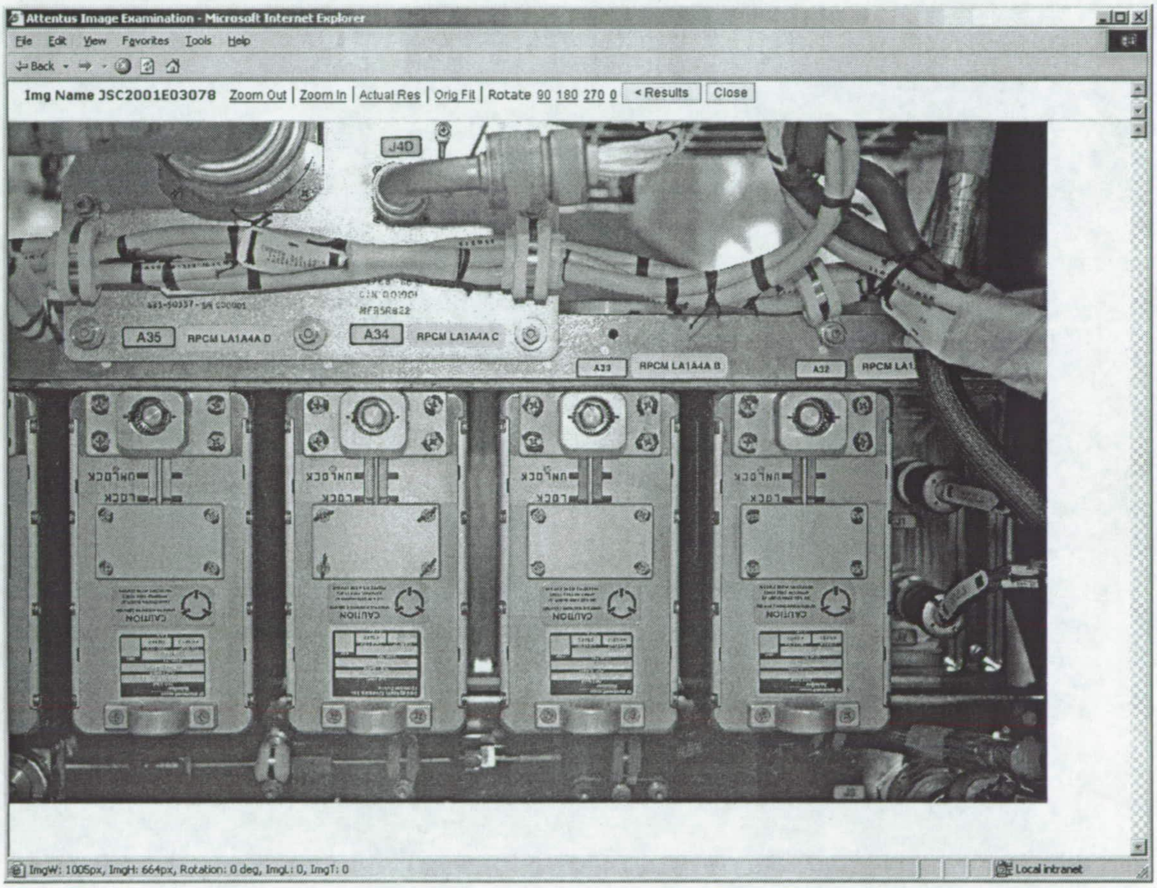

Figure 17.5.2-8. An image of the power controller module shows its configuration in DC converter rack 1. The browser-based controls allow the engineer to zoom in, zoom out and rotate the image for analysis purposes.

Figure 17.5.2-8 shows an image in JPEG format displayed using the web browser as the viewer. Controls to examine the image by zooming in or out or by rotating the image are provided. In this manner, high-resolution digital imagery becomes a valuable artifact for Configuration Management purposes in the product lifecycle.

The technical data management processes, systems and techniques described in this chapter are the result of an evolution that began when the computer age planted the seeds for an infrastructure that would replace drafting boards with integrated digital design environments and slide rules with computer-based modeling systems capable of high fidelity analysis of virtually every physical, economic and managerial aspect of the Space System lifecycle. The steady shift from paper-based engineering artifacts to digital artifacts, and the migration from functionally aligned organizations whose members interact face-to-face to virtual project teams spread across continents collaborating via web-based toolsets has brought about radical changes in how Space Systems Engineering is conducted and how its products and deliverables are created, managed and used.

The net result of this radical shift in engineering processes and products has been to shift technical data management from a back office administrative support function into a pervasive business critical function that translates into a competitive advantage when properly designed, constructed and executed. Those who understand its potential leverage it to deliver the seemingly impossible; those who ignore it risk failure in even the most mundane – how do you deliver schematics when your server has crashed and your customer has long ago retired their print shop?

REPORT DOCUMENTATION PAGE			*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YYYY)*: 5-28-08

2. REPORT TYPE: Book Publication

3. DATES COVERED *(From - To)*:

4. TITLE AND SUBTITLE: Applied Space Systems Engineer - Chapter 17 Manage Technical Data

5a. CONTRACT NUMBER: NNJ06VA01C

5b. GRANT NUMBER:

5c. PROGRAM ELEMENT NUMBER:

5d. PROJECT NUMBER:

5e. TASK NUMBER:

5f. WORK UNIT NUMBER:

6. AUTHOR(S): Peter Kent

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES):
United Space Alliance
8550 Astronaut Blvd
Cape Canaveral, Fl 32920
USK-T26

8. PERFORMING ORGANIZATION REPORT NUMBER:

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES):
Department of the Air Force
Headquarter United States Air Force Academy

10. SPONSORING/MONITOR'S ACRONYM(S):

11. SPONSORING/MONITORING REPORT NUMBER:

12. DISTRIBUTION/AVAILABILITY STATEMENT:

13. SUPPLEMENTARY NOTES:

14. ABSTRACT

This chapter presents the key aspects of Technical Data management within the Space Systems Engineering process. It is written from the perspective of the System Engineer tasked with establishing the Technical Data Management process and infrastructure for a major project

15. SUBJECT TERMS

Technical Data Management
Space Systems Engineering

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Peter Kent
					19b. TELEPHONE NUMBER *(Include area code)* 264-8400