A Multi-Model Approach for

Deriving Requirements Specifications for a Mega-Project

C. (Baba) Piprani, Project Senior Advisor
Colonel R. Bruce Morris, Project Manager[1]

Canadian Forces Supply System Upgrade Project
Department of National Defence
Ottawa, Canada

Abstract. This paper illustrates the experiences in the adaptation of the Conceptual Schema approach as defined in ISO TR 9007 on a mega-project. It steps through the stages that a large project for the re-design of a secure networked Automatic Data Processing system takes in a particular Canadian Government Sector. The experiences of personnel in establishing the necessary framework for requirements definition and specification are highlighted. Traditional large information technology projects present their requirements in elusive terms, using narrative text for contractors to analyze. The Canadian Forces Supply System Upgrade Project has taken an innovative approach in formalizing its system specifications for presentation to contractors. The paper defines the framework of models that were used in establishing the set of system specifications and its associated problems with people, skills, time and resources, in terms of Conceptual Schemas, Database Semantics, and Databases, to handle a mix of classified and unclassified data. This is the first time that a large government project in North America is approaching industry with a formal specification suite based on a comprehensive set of integrated models. This paper summarizes the work done in this area to the time of submission of the responses to the Request for Proposal for Funded Project Definition phase of the Project (August, 1991).

---

[1] **Mr. Piprani** has been involved in a senior capacity with the Canadian Forces Supply System Upgrade Project since 1984, where he introduced Natural-language (Nijssen's) Information Analysis Method (NIAM) to the Project. Prior to 1984, he was a senior Data Management Consultant with Control Data Canada Ltd for 13 years, consulting and teaching NIAM, consulting and implementing applications using DBMS adaptations of the NIAM based models. His background includes a bachelor's degree in Mechanical Engineering, Post Graduate Diploma in Industrial Management (equivalent MBA) from the University of Madras. He was also teaching at both Control Data Corporation, Massachusetts and at Northeastern University, Boston, where he pursued his graduate work in Industrial Engineering (MS). He has been actively involved in ISO Working Groups for Conceptual Schemas, Database, Open Distributed Processing and Database Language SQL2. He is also an active member of IFIP 2.6. **Colonel R. Bruce Morris** is the Project Manager. His background includes being the Director of ADP Operations for the two National/Departmental Level Data Centres at Canadian Forces Bases Borden and Ottawa, and several technical communications-electronics positions prior to being appointed Project Manager in 1988. The authors wish to thank Mr. Maurice Smith, Dr. Robert Meersman, and Dr. T.W.(Bill) Olle for their contributions in some enlightening and "lively" discussions in this area. The authors also thank the Canadian Department of National Defence, for allowing publication of this paper and support from the CFSSU Project staff, in particular the Project Director, Col. Ralph A. Genest, and the senior staff of the Project Management Office. This paper reflects the opinions as expressed by the authors and does not represent the official position of the Canadian Department of National Defence.

1 Introduction

1.1 Situation

The Canadian Forces Supply System (CFSS) provides logistic support to the Canadian Forces situated in Canada, Europe and other nations where Canada is involved in UN peacekeeping and NATO operations. The CFSS is currently integrated as one supply system servicing the Land, Air and Sea Operations of the Canadian Forces and the Department of National Defence. These three services of the Canadian Forces were themselves unified in 1969 from three separate entities. The Canadian Forces Supply System Upgrade (CFSSU) Project is a Government of Canada, Department of National Defence (DND) Major Crown Project. The CFSSU Project was initiated in March 1981 to design and implement a new Canadian Forces Supply System (CFSS). Its mandate is the re-design of the supply system based on the introduction of a new inventory management concept using Distribution Resource Planning / Manufacturing Resource Planning concepts. The CFSSU is a $250 million project that is scheduled for implementation between 1994 and 1997.

1.2 Objective

The objective of this paper is to provide an overview of the Project's initial approach to the provision of a set of formalized set of system specifications based on the Binary Relationship Model of the functional requirements. The paper emphasizes the relevance of the Conceptual Schema approach for the Project's Universe of Discourse and defines a framework of models that were used in formalizing the system specifications for presentation to contractors, to be used during a partially funded competitive project definition phase for the preparation of priced implementation proposals.

2 Background

2.1 The Current CFSS

The current networked ADP system was made operational in 1974 under IBM's Data Base Data Communications Information Management System (IMS) Database Management System (DBMS). Prior to this time, the operations were manually controlled and/or through cards and sorting machines. The design of the current CFSS was begun in the late 1960's under the DEVIL (*DEV*elopment of *I*ntegrated *L*ogistics) Program. Using traditional analysis and development methods, this Program at one time involved up to 1200 personnel. It was difficult to manage and coordinate this large number of analysts. DEVIL also had too ambitious a scope to accomplish. In the early 1970's, the program was cut to its absolute minimum functionality, and using the newly introduced IBM IMS Database system, development of CFSS Application Programs began in 1971. The central host computer configuration, based on IBM compatible configuration under MVS, has been kept relatively current in its hardware and systems software configuration items.

2.2 Major Problem Areas

Since its introduction in 1974, more than 7000 changes have occurred as a result of new functionality requirements, configuration item upgrades, or bug fixes. System documentation has been either sparse or not available. Nearly a million lines of COBOL code exists that are largely without the required functional or technical documentation. The system processes over 100,000 IMS transactions in a given business day and is operated out of the central host computer at Canadian Forces Data Centre Borden in Canada. The current Supply System is inflexible and is not easily understood by its users. The CFSS development required adaptations or extensions to IMS and used a short-lived communications protocol (IBM 2770 was alive in the market for less than 6 months), and resulted in hard-coding many embedded parameters in the application programs. This has resulted in interdependencies and duplications of application programs code with severe impact on the ability to make any changes. The known application backlog is usually over 3 years. Several steps are under way in modernizing the applications in terms of generic I/O and database modules, cross-referencing and dictionary residency (the current Data Dictionary/Directory System is passive, for documentation and data resolution only).

2.3 Need for a New CFSS

Over and above this, the existing system was designed for peace based on a supply "order point" concept, and is difficult to adapt to changing dynamic requirements and for addressing pressing operational matters like the recent Persian Gulf activities. It was essentially designed to address a static reactive environment, with no capabilities for look ahead or for addressing requirements in a proactive fashion. There were urgent requirements to address dynamically assigned flexible supply and repair networks based on new inventory management concepts. There were other requirements that also needed to be addressed in the changing times for providing ADP support to first line units in the field and at sea. Recognizing the 10-15 year general life cycle of the ADP system, the CFSS Upgrade Project was initiated in 1981 to address the new requirements.

3 Approaches for Requirements Analysis

3.1 Traditional Analysis Approaches

After having concluded that upgrades were not only required to the IBM customized-for-DND hardware terminals and the central processors, but that functionality itself had to be addressed, the search began for compatible Commercial-Off-The-Shelf (COTS) software that could be adapted. Not having much success, the search extended to the use of analysis techniques for System Development. A set of requirements were drawn up using traditional Function Modelling and Process Modelling techniques (De Marco, Gane & Sarson) in 1982. These were found to be too informal and the resulting products were very ambiguous as a basis for Systems Specifications. The Project definitely wanted to avoid the previous scenario of bug fixing after implementation. It was concluded that traditional systems development methods did not provide a safe platform for systems development.

3.2 Conceptual Modelling using Entity Relationship (ER) Approach

Chen's Entity Relationship (ER) Approach was used in 1983 to develop a set of functional specifications which could be provided to contractors for implementation of the CFSSU requirements. Military Functional Analysts involving a broad range of personnel from officers to non-commissioned members were trained along with assisting Data Processing computer analysts as cohesive teams. A controlled problem area was developed by two separate teams that presented their analysis results in the form of an ER model. The results were difficult to consolidate and integrate. Measuring overlaps presented a problem since there were no rules for defining Entities, their Relationships, or their Attributes. On examination of the two models on the same subject area, one could not definitively state that they were addressing the given subject area. There were too many ambiguities in the business rules, the basis of the analysis process was ad hoc, business rules were still buried in narrative text, and, there was difficulty in adhering to a standard with several sub-teams since there was no defined approach to identify what constituted an entity, or what constituted a relationship, or what constituted an attribute.

3.3 Conceptual Modelling using NIAM

The Project migrated to a Binary Relationship approach [1] using Natural-language (Nijssen's) Information Analysis Methodology (NIAM) [2] as its modelling approach in 1984. The NIAM approach was supported by Control Data Corporation's Information Analysis Support Tool (IAST) suite of products. Project team members made up of a mix of military personnel (representing subject matter specialists) and civilian personnel (representing the modellers/prototypers) were trained in

NIAM. The business analysis, using functional decomposition techniques, identified 14 major business activities to represent the major supply functions ranging from Administration of Accounts, Materiel Tracking and Warehousing, Order Materiel, Plan and Schedule Materiel, Forecasting, Inventory Planning, to Financial and Procurement Planning. After initial scoping, NIAM Information Models for each of the identified supply functional areas were built. NIAM offered an unambiguous approach to defining the semantics of the functionality requirements. Because of its strong typing, formal business rule declaration, differentiation between things and names of things, sub-typing and inheritance, the Project was in a position to conduct a paper prototype of two large sub-models (Materiel Tracking and Accounting, and Inventory Management and Planning) for the purposes of identifying overlaps and interface requirements. A six month exercise of defining the two separate models provided conclusions that these two could not be transitioned and implemented independently from the current CFSS, and that what was at one time thought to be a loosely coupled interface turned out to be a very complex inter-related requirement. This meant that the two major sub-systems could not be piggy-backed sequentially in transition or implementation from the current system to the new. This was a very valuable exercise that also demonstrated that the current IMS system structure could not be modularized neatly for purposes of transition or staged implementation. The business rules in the current system were buried in many application programs and intertwined. But, this exercise also provided the necessary platform for the start of system transition planning.

3.4 People and Organization

The bringing together of the Functional Analysts (user proxy) and Technical Analysts (modelling assistance) worked well initially. The Functional Analyst represented the subject matter expert and was knowledgeable in NIAM, being at least able to understand and read the same language as the Technical Analysts. The Technical Analysts, because of their data processing background, were to be in a position of being the modellers. NIAM training was conducted every year to accommodate the high rate of personnel changes. However, because a limited time was spent on the formal training of either functional or technical analysts, and because of people turnovers (military personnel have an average three (3) year posting cycle, and civilians wish to maintain career progression), the strong team bond was difficult to maintain, and skill levels in several sub-teams was at varying levels. The results of this was apparent in the Quality Assurance Reviews. The objective was to have the Technical Analyst develop the models with the assistance of the Functional Analyst, each using the same language, i.e. NIAM. There were two major teams, one for the Materiel Tracking sub-model, and one for the Inventory Management sub-model. Each of these had between 4 to 6 sub-teams under it, each having one or two military personnel, and one civilian analyst. The Project has had 35 military and 22 civilian personnel over the past seven (7) years, with an average of about 60% dedicated to deriving the functional requirements using modelling approaches. The proportion was closer to 80% until 1989 when personnel resources, within the same total, had to be converted to address the system engineering aspects of development of the broader System Specification for the acquisition process, and the more rigorous project management framework of work breakdown structures and financial breakdown structures for improved control over the actual versus the approved plan schedule.

3.5 Methods and Quality Assurance

Each sub-team developed the initial Business Activity Model (BAM) based on a functional decomposition of the 14 major supply functions and the associated NIAM information models. Standards and Standing Operating Procedures were established for the Project to force a uniform approach for naming and syntax, do's and don'ts, change control and integration procedures, impacting procedures etc. It must be noted that the overall analysis process for this Project was not formally documented to an adequate degree, and was permitted to evolve in a somewhat ad hoc fashion. Indeed, that process continues to evolve as continuing improvements are introduced. The team leader arranged for a peer level review either by his/her team manager or a parallel team. Sometimes this is done using "unrestricted" NIAM, i.e. the development of the models might not have followed, precisely, Project NIAM standards that did exist. There is one corporate NIAM information model. Each of the sub-models were quality-assured at the team level prior to being integrated. The aggregate impact on the corporate model was analyzed. A final Semantic Model Review was performed for identifying overlaps, establishing consistencies and removing redundancies, checking for standards conformance, etc. This final review required NIAM and modelling expertise, and involved the Project Senior Advisor, assisted by the Senior Technical Analysts. Experience has shown that there is always some repair work on the models that has to be done in this "final" review. This aspect has to be recognized and has to be built into the work planning estimates.

3.6 Project Management and Work Breakdown Structure

The Project started under the auspices of the Project Director (representing the Sponsor), who is responsible in leading the project to develop the statement of functional requirements. The Project Manager, representing the facilitator and engineering side of the house, picks up from the Project Director, and develops the system specifications to be made available to contractors. The Project Manager provides the system engineering design authority input for the entire CFSSU system infrastructure requirements. The Project Manager establishes the processes for selection and evaluation of contractors, procurement, implementation, acceptance and initiation of in-service support. After successful acceptance, the Project Manager then delivers the system to the Project Director, who then becomes responsible for in-service support and maintenance. Since 1989, the Project has been under the Project Manager. The Work Breakdown Structure (WBS), a list of activities and tasks that need to be performed in all Project areas, including the sections for analysis using NIAM, is employed. This is an area that requires judicious regulating, since at one time the Project found itself spending 60% of its time administering itself rather than getting the definition and analysis work done. Following the textbook approach, work is scheduled as per the WBS. As it often happens on a modelling project, estimating the complexity of the model has a high degree of uncertainty. Experience has shown that abstraction is a difficult process to estimate. NIAM at least provides the linguistic platform on which to build one's analysis. This is often used to decide upon the number of concepts, fact types or sentence types, each of which represent a statement of supply business policy. The resource and time estimates are also dependent on the "average" modeller, an entity which does not exist. Since modelling is an iterative exercise, the question often arises as to where to stop! If the rate of introduction of new NIAM Information Model concepts i.e. each Non-Lexical Object Type (NOLOT), Idea Type (IDT) etc. is monitored against time, the flat-topping of the rate of introduction gives an indication that the model is near stabilization. In the Process Modelling realm, since the majority of processes are Information Model derived, each User Task was to have been categorized in the "Simple (S)", "Moderately Complex (M)" and "Procedurally Complex (P)" for purposes of estimating effort. An S task had no conditionals and was a straightforward in-out database operation. M tasks were to have had some conditional retrievals, IF's etc, with total number of conditions less than 10. P tasks were to have had greater complexity and were usually to have been procedural, often with importation of statistical algorithms etc. This functionality breakdown was expected to have given a better handle on the estimating complexities with many variables. In summary, estimating modelling efforts on a large project has shown to be very elusive, particularly because of the mix of modelling skills required. A 20% contingency factor was eventually mandated to be built into every work plan estimate, and it was recognized that even the final QA review of the NIAM model could unearth hidden constructs that were required, but not recognized earlier. This latter effect is much more common on a large complex project employing modellers of varying skills.

4 Project Definition and Procurement Strategy

4.1 Single Contractor versus Funded Project Definition

Because of the nature and size of the Project ($250 M with more than 3500 terminals envisaged), a unique procurement strategy had to be developed. It is normal practice in the Government of Canada to have a two stage approach for information technology procurements. The first stage involves defining the requirements called, Definition, where the system specifications are developed based on the approved functional requirements. The second stage involves implementation of the system specifications to result in a system that is constructed and implemented compliantly. Each stage is usually done by separate contractors i.e. the same contractor is not allowed to bid on both the stages. Because of the complexity and size of the CFSSU Project, this approach was seen to represent a high risk with a high degree of disconnect---the second contractor would be blaming the other for any aspects of non-compliance. More importantly, the knowledge, skills, and government-contractor teamwork developed in the first stage were lost, with the implementation contractor having to be educated and trained in the project's environment. Special waivers were sought to be able to have the same contractor proceed with the two stages. This would have meant that the preliminary selection would have been fraught with danger and high risk. Selection of a less competent or non-competent "low-ball" price contractor could have proven fatal. It was decided to partially fund the first definition phase called the Funded Project Definition phase, wherein two qualified contractors would be selected to each submit a comprehensive Implementation Proposal. The phase for the preparation of the priced implementation proposals was estimated to last one year. Each of the FPD contractors would be provided $4M towards this phase, and it was estimated that the work involved would easily cost the individual contractor at least an equal sum as part of each participating contractor's investment costs. Selection of the prime contractor would then follow after a three to six month bridging phase for evaluation and Canadian Federal Government decision. A firm price contract is envisaged, while other options such as target incentive within a ceiling price for the high risk software development area are being permitted. Implementation and full design would begin after selection of the single contractor. It is important to note that there is only "negative guidance" provided during the FPD phase. By this it is meant that, beyond the usual mechanism to identify perceived errors of omission or commission and to seek clarifications, the contractors would be told that they would likely be non-compliant if they were to follow a particular route as observed during the informal on-going progress reviews. But they will not be "positively" told what to do. This is to avoid unfair treatment between the two contractors. This strategy requires that the system specifications given to the contractors be complete, formal and precise. This is what the CFSSU Project Management Office is committed to prepare---NIAM-based functional specifications to be provided to the two FPD contractors as the basis for the preparation of their priced implementation proposals. Figure 1 illustrates the CFSSU Project Life Cycle, including the several versions of the system specification that are required. The CFSSU Project Management Office has had extensive interactions with eligible potential prime contractors in the form of Industry Briefings [3, 4], followed by bi-lateral sessions during the summer of 1990. That consultative process continued with the provision of the draft Request for Proposal in October, 1990, and the first Specification Orientation Seminar in May, 1991 following the provision of the Request for Proposal.

4.2 De-scoping the Project

It has been often mentioned in the news media that large "grand design" projects are at high risk. The CFSSU Project has had several spin-off projects in terms of immediate terminal hardware replacement for the original customized terminal hardware set to keep the system operational, the Cataloguing of NATO items, the Sub-projects for Inventory Reporting etc. What remains is the basic core of supply requirements that has been modelled in NIAM and represents the irreducible set of functionality required by the Canadian Forces Supply System. One other way of reducing the risk was to approach the area of system specifications with a formal approach---in terms of modelling the requirements themselves, and modelling the formalizable functional specifications around the requirements i.e. after having defined the Universe of Discourse for the CFSSU, a Conceptual Schema based approach of modelling the requirements and the functional specifications was undertaken. Under part of the original Project Definition funding in the mid-1980s, an option analysis was done in terms of re-engineering the current IMS-based CFSS into either IMS itself or on an International Organization for Standardization (ISO) Standard SQL-based DBMS platform. The quality of the existing functional and technical documentation of the current system internals was insufficient. Hence, it was considered to be too risky to venture into the current system internals---particularly when a good portion of the order point based programmed functionality was deemed obsolete and not required for the new planning and scheduling concept. Deriving an SQL-based model from an IMS data structure model without meaningful semantics would prove to be unworkable, or, would cost several times more than modelling a new requirement properly. This is not to preclude any efforts at reverse-engineering or some forward engineering of the current CFSS. Any such efforts will only improve the baseline for on-going support and for the data conversion and system transition to the upgraded CFSS.

4.3 System Specifications for the Contractors

Because of the nature of the "negative guidance" during FPD, it was a requirement that the Project would provide unambiguous and a complete functional specification set for the two FPD contractors. As of December 1990, after providing a draft version of the Request for Proposal to the eight (8) eligible potential prime contractors in October, 1990, it was the Project's intent to provide the FPD contractors a set of completed NIAM models as background information (non-mandatory), and their representation in a logical data model based on ISO SQL2 DDL as mandatory. This meant that the functionality and semantics as described by the ISO SQL2 DDL in terms of database structures, business rules in table and column constraints would have been required to be implemented. The contractors could have been free to superimpose other data structures for purposes of optimization and distribution etc. For the Process Model and dynamic aspects, Information Flow Diagrams [5] and associated Process Model descriptions would have been provided to accompany the SQL2 DDL. These would have been mandatory in terms of meeting the required functionality also. These two only represent the Functional Specifications portion of the system specification set. Other specifications are addressed in a later section of this paper. The SQL2 DDL was designed to be automatically generated from the NIAM model using Control Data Corporation (CDC) IAST tool set and an in-house suite of application programs (called IAST+) to handle gaps in the IAST suite. As a start, a subset of ISO SQL 89 was generated for October 90's version of the draft Request for Proposal for the selection of Funded Project Definition contractors. The undocumented complexity of the IAST meta-schema and time/resource constraints, with the additional load of generating cross-references between NIAM and SQL2 columns, were factors that contributed to a revising of the decision of the Project on its specification components. The Project has now provided the Contractors with NIAM models and the Information-Oriented Process Models as representing the Functional Specifications in its purest form. The following paragraphs describe some of the specification components in this and other areas, as they were used for the Request for Proposal.

5 The Framework of Models in the CFSSU Project

5.1 The Models of the Functional and Operational Specifications

The CFSSU Project Management Office has opted to take a formal approach using modelling techniques for the definition and conveying of semantics of the different requirements. While several systems development methodologies and approaches exist, experience has shown that every project is different. There are some things that are always different and this is what makes each project unique. It is necessary to adapt other methods, or develop new methods to fit it into a general life cycle model, and to convey a unique set of requirements. Because of the nature of the complexity of the CFSSU Project, and its advanced state of system specifications, accompanied by the unique FPD two-contractor negative guidance approach, the Project has identified a comprehensive list of specifications. Figure 2 illustrates the positioning of the different models with respect to each other and provides a high-level view of the connectivity amongst the models. Each of the involved models are briefly explained below, and the list of specification components includes outputs from each of the models. These are described in the following paragraphs.

5.2 NIAM Information Model

This model depicts the Information Model using the Binary Relationship approach in terms of the following NIAM concepts:

- Non-Lexical Object Types (NOLOTs)
- Lexical Object Types (LOTs)
- Idea Types (IDTs)
- Bridge Types (BRTs)
- Constraints---
    - Uniqueness
    - Exclusion
    - Total
    - Joint Uniqueness
    - Joint Total
    - Procedural (including cardinality and ranges)
    - Derivation Rules
    - Defaults
    - Privileges

The above concepts are resident in the CDC IAST Dictionary which allows the entry, manipulation, reporting and graphic representation of the model. The semantics of the model are portrayed by means of an Information Structure Diagram (ISD) and associated constraints list.

5.3 Information-Oriented Process Model (Adapting NIAM)

This model depicts the Process Model in the form of a Business Activity Model, using Event-driven analysis and User Tasks. A User Task is seen as fulfilling a functional requirement e.g. Opening of a Customer Account. The minimality condition of this is governed by the Information Model business rules and constraints that require certain minimal actions to be performed on the database for integrity reasons. The upper limit is usually the activity to be performed as a result of an event action in the environment. As mentioned in the Project Management and Work Breakdown Structure paragraph 3.6, User Tasks were categorized by degree of complexity in S, M, and P types to facilitate breakdown of work both for the Project and for the Contractors. This was to have also assisted the Contractors in identifying the kind of resources required and complexities in estimating the Application Architecture configurations, since estimates of S&M User Tasks become linear. Component Processes were defined on the NIAM Information Model Idea Types based on the minimality condition as stated above by each Non-Lexical Object Type. The Component Processes were NIAM Information Model derived processes and special non-Information Model derived processes. Each of these processes was built on a canonical operation of a Create, Retrieve, Update, or a Delete, and, each one of these was re-usable. The Interaction Model established the connectivity and control structures from the User Task to the re-usable Component Processes. A formal link existed between the NIAM Information Model and the User Tasks in terms of NIAM Binary References via the involved Component Processes. Because of the advanced nature of this model, relative to the capabilities of the IAST suite of tools, only parts of it resided in IAST for formal connection to the NIAM Information Model, while parts of it were external, within the Project's extended suite of products (known as IAST+).

5.4 Operational (Requirements) Specifications Model

This model depicts the Supply User Operational Requirements in terms of volumetrics by location, for User Task activity, User Task complexity, frequency of invocation, recoverability, degradation mode, messaging requirements, with a planned provision to address differences in the modes of operation in terms of war, peace, emergency, and mobilization. The model itself consists of definitions of applicable SQL table formats accompanying the table populations for the different locations and associated parameters. The SQL model is derived from the NIAM Model for the Operational (Requirements) Specifications. The populations represent the values that the contractors will be using to develop their general system design and architectures.

5.5 Access Control and Authorization Model

This model depicted the Access Controls required for Persons, Positions, and Occupational Groups against the User Task Groupings for given sets of general duties and work patterns. Applicable User Task Authorizations were also recorded towards meeting the Department of National Defence's policies and standards on management controls and auditability. The SQL model was derived from the NIAM Model for the Access Control and Authorizations. The populations represented the values that the contractors will use in developing their general system design and architectures for Access Control and Authorization. This model would also represent the specification for the requirement to develop the associated Access Control and Authorization Model Services by the contractors. Each User Task (see 5.3 above) was envisaged at that time to be invocable only through a derived menu that is appropriate to the given access level.

5.6 Data Sensitivity Model

This model depicted the combinations of data elements and associated values either by themselves or in aggregate that make the set sensitive for either national security or other sensitivity (e.g. designation for protection not for national security) requirements. Although a given User Task and associated menu entries could be invoked dynamically, data sensitivity would inhibit/override the actual invocation of the User Task with the selected database values. The SQL model was derived from the NIAM Model for the Data Sensitivity Model. The populations represented the values that the contractors would use in developing their general system design and architectures for Access Control and Authorization, and Data Sensitivity. This model would also represent the specification for the requirement to develop the associated Data Sensitivity Model Services by the contractors.

5.7 Conversion and Mapping from Current System Model

The mammoth and often underestimated task of transitioning from an existing system to a newly developed system presents an extremely difficult situation. This model depicted the mappings from the NIAM Information Model to the IMS Data Elements used in the current CFSS in terms of Data Mapping. The Process side was also mapped with the User Tasks in the CFSSU against the current CFSS Transaction Interchange Code (TIC) structure. This functional mapping was performed against the applicable business rule checks and edits as shown in the current application programs. The conformity or discrepancy of the mappings were recorded in the populations of this model. The SQL model was derived from the NIAM Model for the Conversion and Mapping Model. The populations represented the values that the contractors would use in developing their Transition strategy and the design of special configurations for Transition and Mapping . This model would also represent the specification for the requirement to develop the associated Conversion and Mapping Model Services by the contractors.

5.8 Transition Differential Model

This model depicted the differential thresholds in terms of limitations and constraints that are to be applicable during transition from the current CFSS to the upgraded CFSS. This is particularly important in terms of the variability of data values possible due to the different approaches in inventory management being introduced (i.e. the switch from order point concept to a planning and scheduling concept). Permissible and non-permissible ranges/thresholds were planned to be used to establish inner and outer time periods that would enable derivation of go/no-go time windows for transition. The SQL model was derived from the NIAM Model for the Transition Differential Model. The populations represented the values that the contractors would use in developing their Transition strategy and the design of special configurations for Transition and Mapping.

5.9 Configuration Management System Meta-model

For effective understanding and control of the CFSSU Project's numerous inter-related specifications and their parts as they go through the various stages of their existence, a meta-model (or n+1 level model) of the configuration management objects and associated processes was developed. This meta-model defined and described the configuration management components and processes that would deal effectively with both documents and Computer Software and Hardware Configuration Items, and provide traceability through the requirement for the contractor to address these "versionable objects" through some form of Repository Services. It was essentially based on the emerging ISO Standard for Information Resource Dictionary System (IRDS) Services Interface, and defined a framework of components that were deemed "versionable". The SQL model was derived from the NIAM Model for the Configuration Management System Meta-model. The populations represented the values that the contractors were expected to use in developing their Configuration Management Plan and Services, including the design of special configurations for a repository-based system. This model would also have represented the specification for the requirement to develop the associated Configuration Management Services by the contractors.

5.10 Multi-model Approach Examples

This Project's multi-model approach is illustrated in Figures 3, 4, 5, 6 and 7. The right side of each of this set of figures addresses the population instances. The left side of this set addresses the model or type. Sometimes, a model is also an instance and the result of this is a meta-model or n+1 level model. This approach has used concepts defined in ISO TR 9007 and the work in the ISO Reference Model of Data Management, ISO IRDS, ISO Reference Model of Open Distributed Processing.

6 Presentation of System Specifications to Industry

6.1 SQL-Based versus NIAM-Based

As indicated earlier, the comprehensive set of models as depicted above and associated populations needed a delivery mechanism for transfer of the system specifications from the Crown to Industry. ISO SQL2 was originally selected as the preferred mechanism for representation of the NIAM model constructs based on the mapping developed by the Project Senior Advisor, facilitated by his direct involvement in the ISO IEC/JTC1/SC21/WG3 Database Language Working Group. A Logical Data Model structure is readily understood by a contractor, and SQL was used as the formal database structure specification language. As SQL2 contains powerful constructs for declaration of Table Constraints, Column Constraints and Assertions, it was selected as the mechanism for specifying the mandatory requirements for a logical data structure. The SQL2 Model was targeted as a 100 % equivalent representation of the static constraints as depicted in the NIAM Information Model---with dynamics being handled by extended constructs using SQL3. In addition, the aspect of change control required the contractors to communicate their change requests on the Information Model in terms of the Logical Data Model. These change requests could be as a result of errors of omission or commission. These changes would then have to be mapped back into the NIAM model, re-introduced in the NIAM model, and the output SQL DDL schemas be re-generated automatically. This process would have had to be conducted for the two FPD contractors separately. This requirement meant that the Project would have had a difficult time managing the three specification models, i.e. the original version that was released, the Contractor A version, and the Contractor B version. Since the Crown is going out to contract to save time and resources, it was obvious that the overhead of change controls should be on the Contractors and not on the Crown. At that time, there was also an inadequate set of software-based tools available. The overall result of consideration of all relevant factors was that

NIAM specifications were made mandatory instead of the SQL2 DDL as mandatory. A mandatory specification by definition cannot be redundantly specified. Additionally, time and skill constraints required to guarantee the mappings of specifications that are in NIAM to be transferred to both the SQL2 and Process models, are requiring the Project to present the specifications using NIAM. However, the danger here is that the extent of the understandability of the Contractors and their knowledge of NIAM, and the know-how for cost-effective/efficient transformation to a DBMS structure may not be known or apparent at this time. This risk can be reduced by a good lower CASE tool that assures a good fit into a good Repository environment using the meta-model of SQL2 as its interface.

6.2 Computer Aided Software Engineering (CASE)---Where Are You?

Considering that all the NIAM constraints are now transferrable to SQL2, and noting that ISO IRDS is using the SQL2 Data Model (Definition Schema) as its database in its level pair construct, it makes sense to have the semantics of the CASE environment for implementation to be resident in a repository that is at least able to adapt the full SQL2 constructs. The CFSSU was using CDC's Information Analysis Support Tool (IAST), a tool based on NIAM and an "early-bird" CASE tool introduced in the early 80's. Even though it was constructed using the level-pair concept and schema-of-a-schema approach, the undocumented features and lack of documentation precluded the extensibility of such an environment. The CFSSU Project was discouraged at the lack of availability of good, properly designed and modelled, intelligent CASE environments that can maintain, formally, the real-world constraints and enforce them in the generated applications. Furthermore, this disappointment extends to the apparent hesitancy of the information technology industry to address the entire "system" from formalizable foundations rather than just the "software" as part of CASE tools. The Project Management Office is not in the CASE development business, but has had to support extensions to IAST (the IAST+ suite) to meet the essential needs not provided by IAST.

6.3 The CFSSU System Specification Suite

The CFSSU System Specification suite consists of six major parts. The first two and portions of the third specification themselves had models i.e. the meta-model of the specifications, since they are formalizable. The remaining are presented to Industry in terms of documents. In brief, the six specifications are:

6.3.1 Functional Specification. This details the functional requirements in terms of Information and Process Models, with associated supporting models like Mapping, Transition and Access Control.

6.3.2 Operational Specification. This details the operational and performance aspects (e.g. volumetrics, end-user response times, transaction throughput rates, etc) of the system in different modes and environments.

6.3.3 Technical Specification. This describes the required technical, including standards, and performance characteristics of hardware and software components including telecommunications, for implementation of the system. This specification will include the technical details of the Government furnished items to be offered on a mandatory or non-mandatory basis for potential inclusion in the configuration to be bid for the final solution. The mandatory items include the DND Integrated Data Network (X.25 based secure packet switched wide area network). The non-mandatory items include a portion of the Materiel Computer System (IBM 3090-500S) configuration on which the current CFSS is processed, and the Motorola-based terminals and processors of the Terminal Network Replacement installed in 1990.

6.3.4 Security Specification. This specification addresses the broad security aspects of the system in terms of certification and conformance requirements of the system. One should note that the contents of the Access Control and Data Sensitivity Models do not address the full spectrum of security requirements which include security sub-sets for the operating system (Trusted Computing Base), hardware (TEMPEST), and communications (Cryptographic devices for encryption/decryption), and physical and personnel sub-sets.

6.3.5 Integrated Logistics Support (ILS) Specification. This addresses the life cycle support requirements of the system--particularly in the "in-service support" phase, i.e. after implementation. This includes to training needs, both initial one-time and recurring regenerative requirements.

6.3.6 Implementation Specification. This details the requirements, limitations and constraints which apply to plans for conversion and transition to the new system, as well as actual implementation of the system at end user sites, plus a life cycle support facility.

These System Specifications are quality assured throughout the Project life cycle via the CFSSU System Development Control Framework.

6.4 CFSSU System Development Control Framework (SDCF).

Within the overall context of the Project's planning and control structure, the CFSSU System Development Control Framework defines the activities, deliverables, and reviews which enable the technical authority to control the development of the redesigned CFSS from the functional, technical and performance specifications into the complete, integrated, operational system. The purpose of the SDCF is to be the basis for Government insight into and control of a contractor's efforts from a quality assurance perspective. Although the SDCF and a contractor system life cycle management method or system development methodology (SDM) are related, the two are distinct. The SDM defines the processes and procedures for developing a system, including the documentation to be produced. The SDCF specifies the deliverables and reviews, including intermediate products, required by the Crown technical authority for visibility and control. The SDCF deliverables will ideally be based on products which can reasonably be expected to be available from modern SDMs. The SDCF must provide an overall review of the complete set of work requirements. It must provide the basis for developing the consistent and complete Statements of Work (SOW's), (the FPD SOW and the Implementation SOW). It must also include a complete and consistent set of Data Item Descriptions (DIDs) to support the Contract Data Requirements List (CDRLs). With all of this complexity and detail, the SDCF must also provide direction and guidance for the use of the SOW, DIDs and the SDCF as a basis for effective quality control for quality assurance. The CFSSU SDCF is being developed using components from the aggregate of system development standards and specifications from AIS/ADP standards organizations, such as the Canadian Standards Association (CSA), Treasury Board of Canada Information Technology Standards (TBITS), International Organization for Standardization (ISO), American National Standards Institute (ANSI), the National Aeronautics and Space Administration's (NASA) Software Management Assurance Process (SMAP), the Institute of Electrical and Electronic Engineers (IEEE), and the U.S. DoD/Military framework of standards and specifications. The SDCF defines the complete set of work requirements, in terms of the required deliverables and applicable standards and specifications for the design, development, and implementation of the CFSSU, and comprises or identifies:

- description of Work Requirements;
- deliverables within a System Development Deliverables Structure;
- data item descriptions; and
- the guide for employment.

The System Development Control Chart is a diagram (see figure 8) which identifies the deliverables by Project life cycle phase. The Project life cycle has been broken down into the seven stages shown in the diagram. Associated with each stage are specific deliverables, reviews, and audits. The first five stages overlap, and it is recognized that these stages may be applied iteratively or recursively. It is also recognized that the end of a given stage may not be as clearly defined as the outline chart at Figure 8 indicates. However, each major stage will end, for contractual purposes, with a formal review.

7 Concluding Remarks

This paper has illustrated one mega-project's experience in the adaptation of the Conceptual Schema approach through the use of multi-models in several disciplines, for the provision of a functionally-oriented system specification. The models are shown to be integrated together and formulate a comprehensive formalized road-map that one can follow. This provides traceability, auditability and reduces the risk of improper system specifications. The paper also visited several experiences in the areas of project management, people, organization, and communicating with contractors. The end result is that the Project Management Office feels confident that the multi-models do address the requirements where defined, or, at least begin to formally approach this area of specifying the functional requirements. A subsequent paper will describe the improvements made to the framework of the System Specifications in terms of the Functional Baseline as it was provided to the three Funded Project Definition Contractors in September, 1992, and the clarifications necessary throughout the period of the preparation of the priced implementation proposals to be delivered 30 September, 1993.

List of Figures

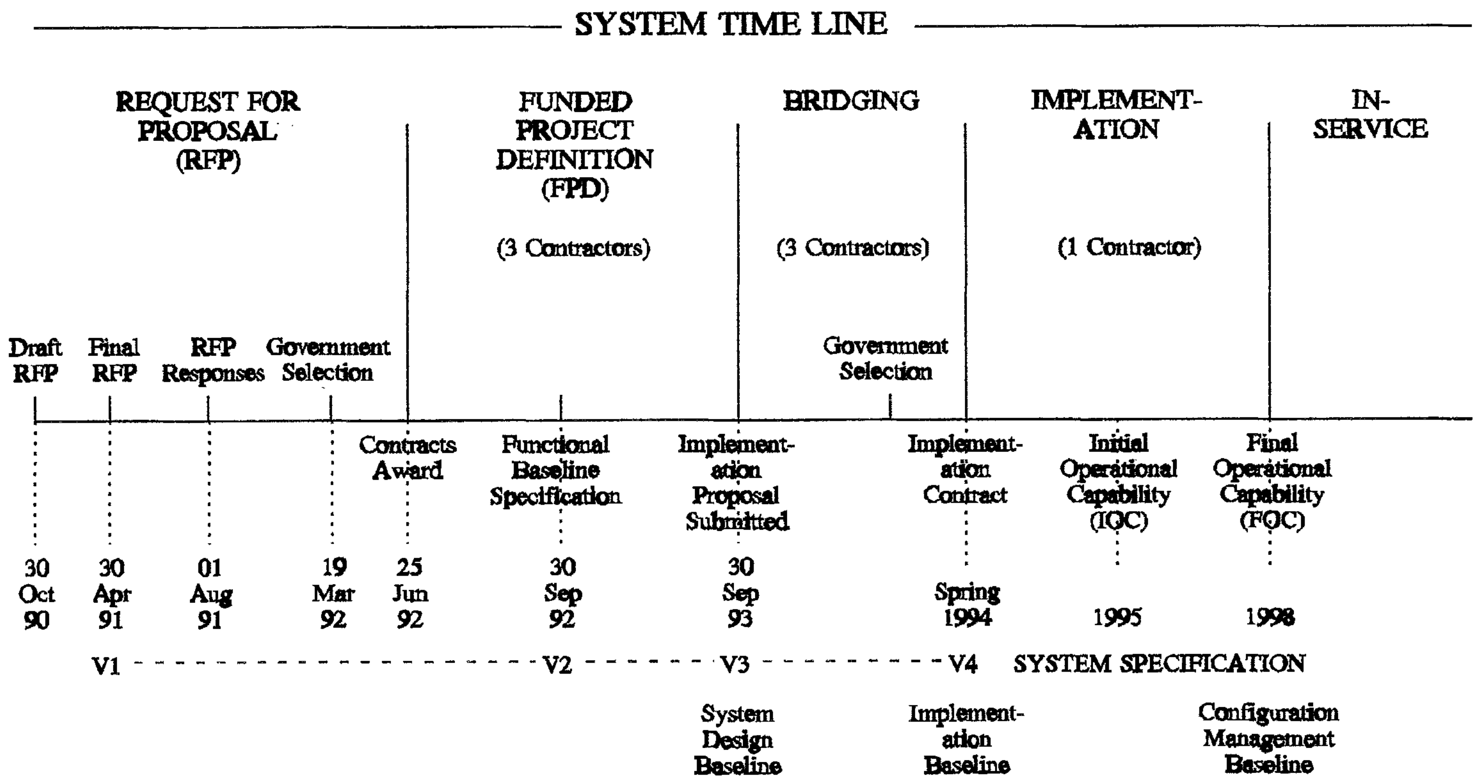


Fig. 1. Partial Project Life Cycle - System Time Line

File # BP93055-2

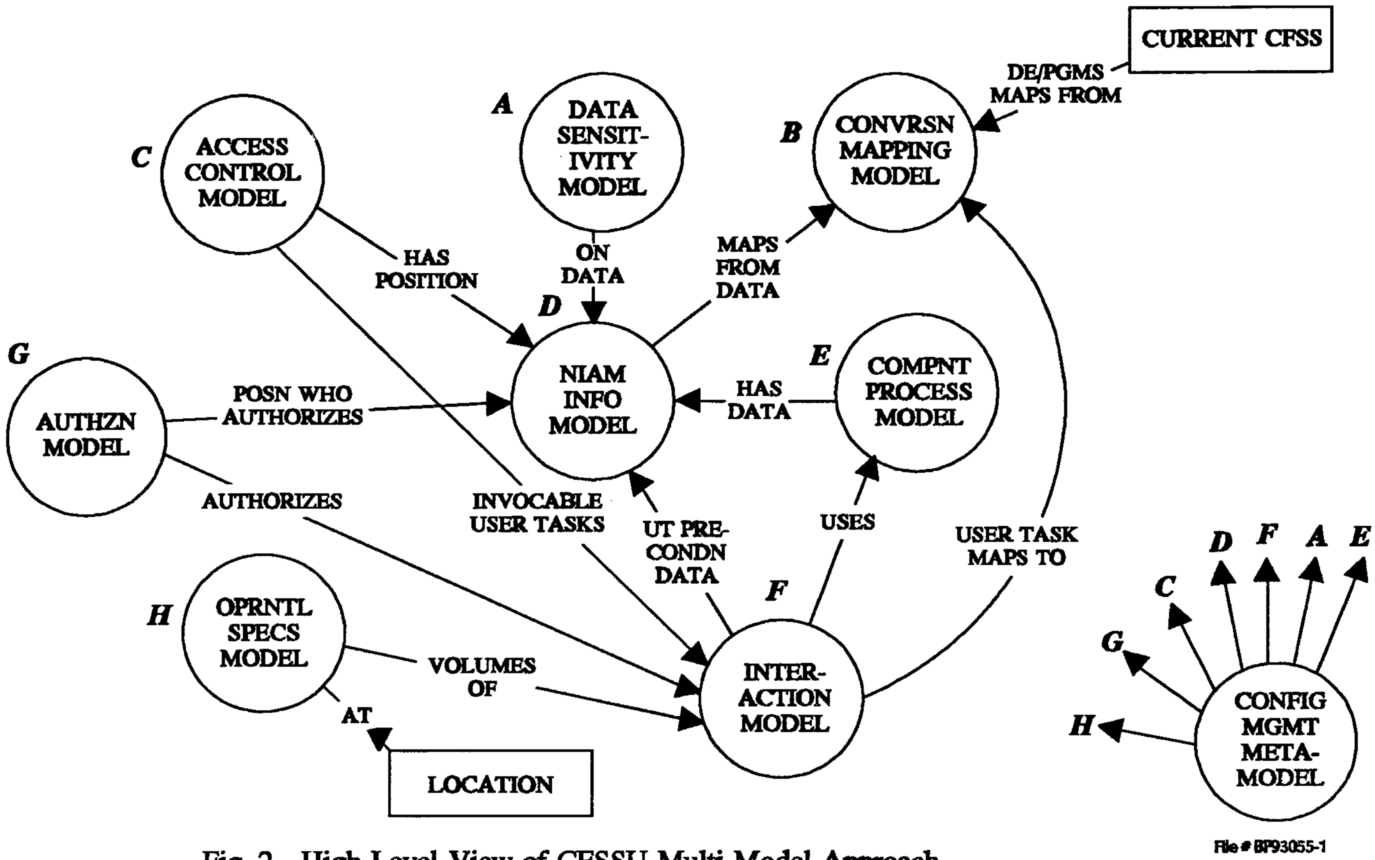


Fig. 2. High Level View of CFSSU Multi-Model Approach

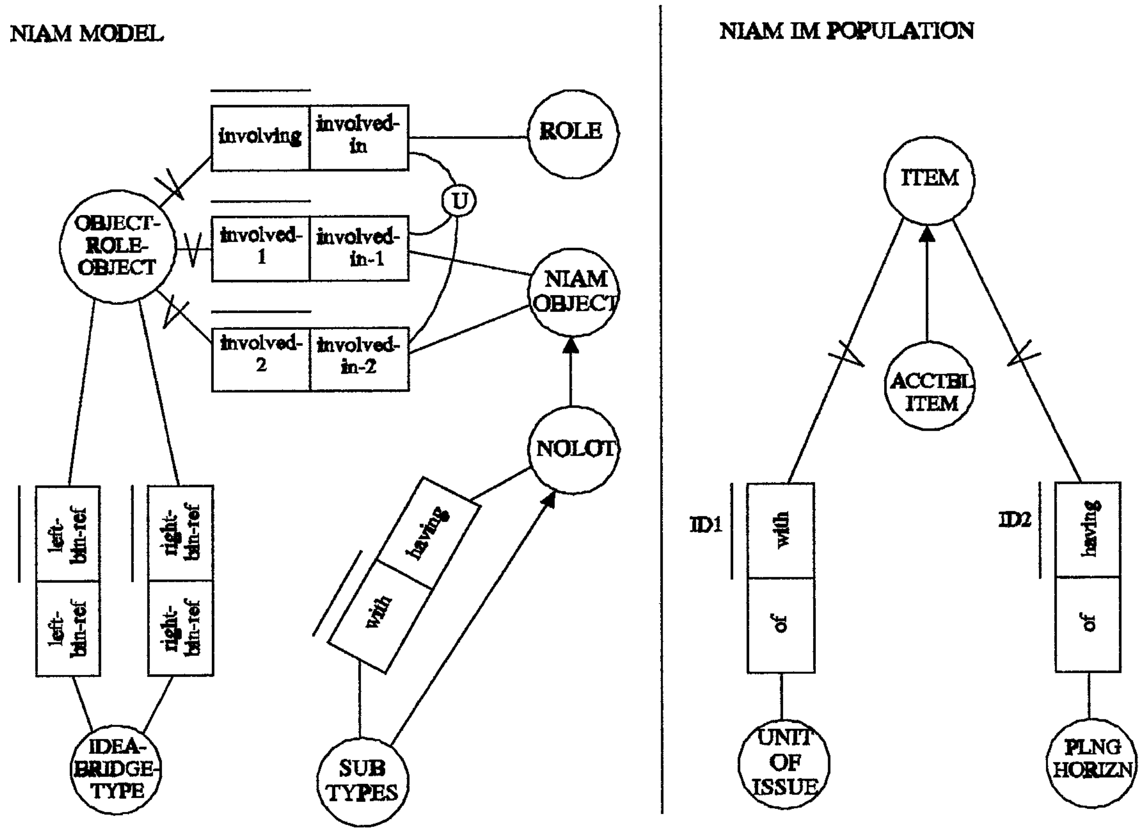
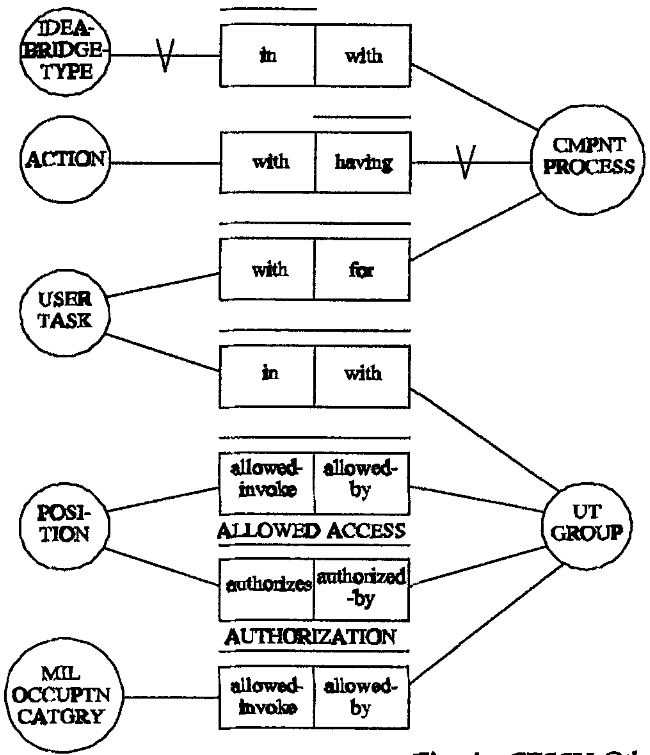


Fig. 3. NIAM Information Model Meta-Model

FILE # BP93049-1



<u>CROSS REFERENCE</u>
<u>USER TASK - BINARY REFERENCES POPULATION</u>

UT1 References IDEA TYPE 2

<u>INTERACTION MODEL POPULATION</u>

UT1 DO Process-P1
UT2 DO Process-P2

UT2 DO Process-P25

UT: Business User Task

P: Re-usable Process

<u>COMPONENT PROCESSES POPULATION</u>

Process-P25

ADD (NIAM Idea Type 25)

<u>ACCESS CONTROL MODEL POPULATION</u>

PERSON 25 allowed invokeUT1

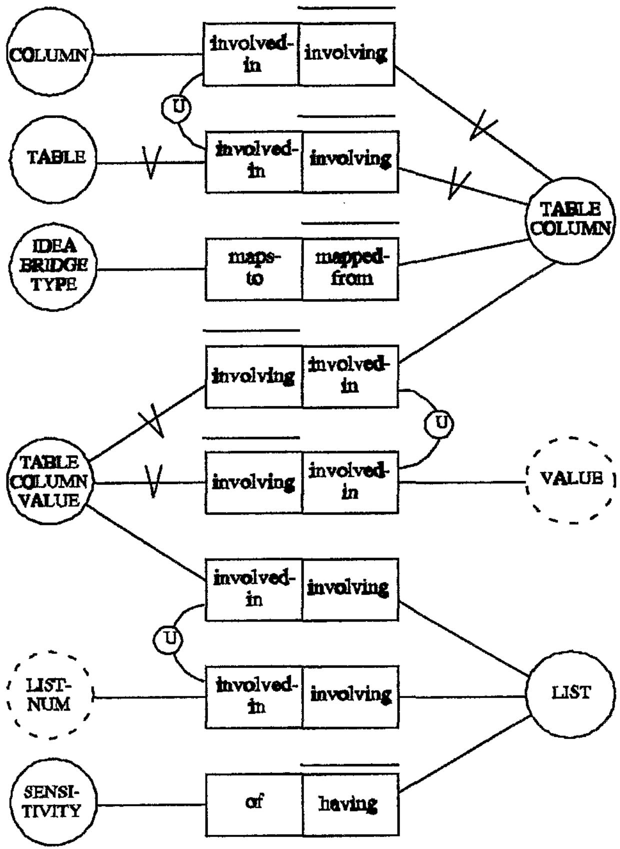
POSITION 16 allowed invokeUT1

<u>AUTHORIZATION MODEL POPULATION</u>

POSITION 25 authorizes UT1

Fig. 4. CFSSU Other Model Representations

FILE # BP93049-2



DATA SENSITIVITY MODEL POPULATION

ITEM-ID 1234 in condn GOOD is SECRET

ITEM-ID 5678 at locn 65 is CONFIDENTIAL

Fig. 5. Data Sensitivity Model

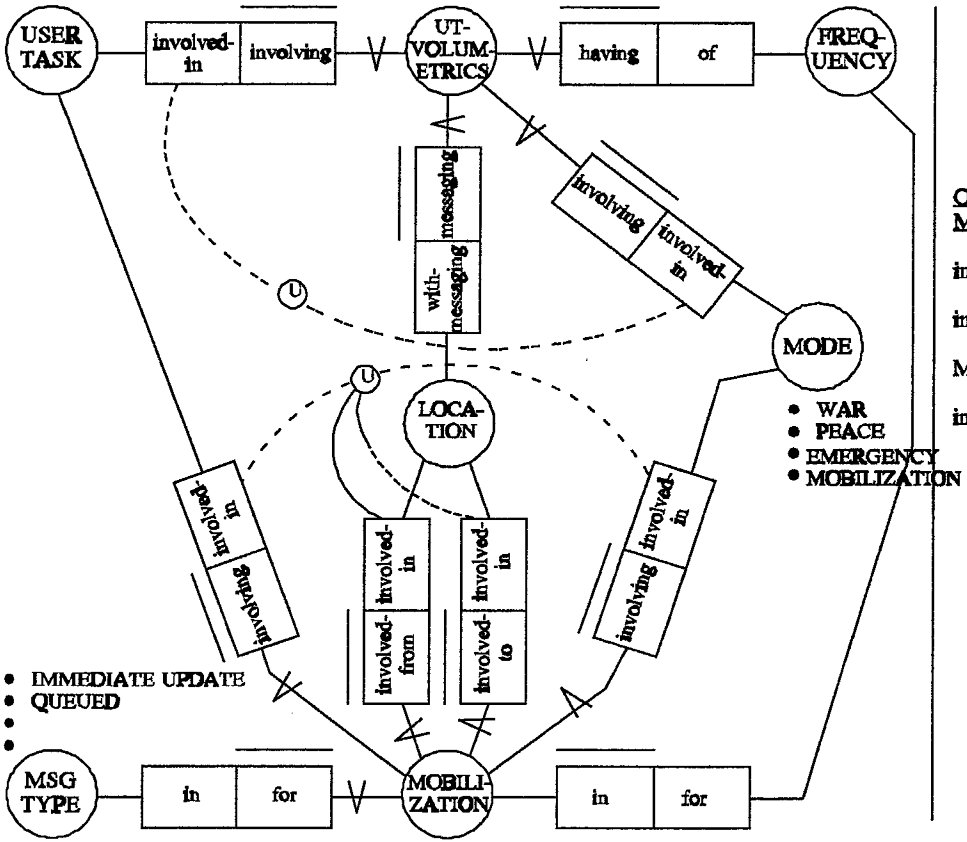


Fig. 6. CFSSU Operational Model

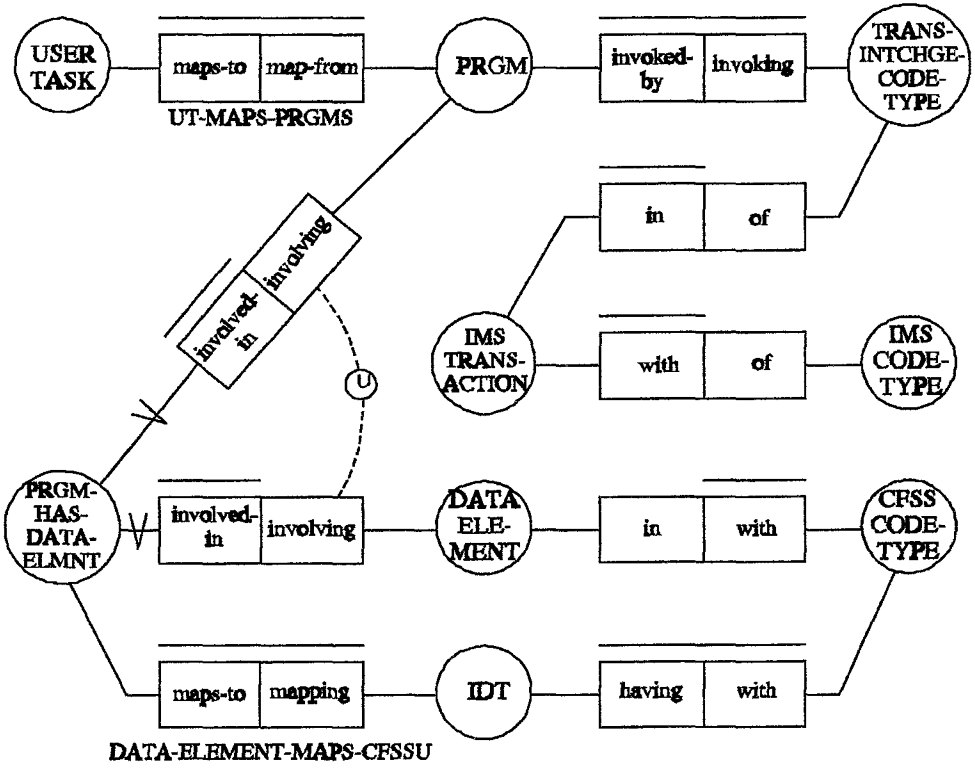
<u>OPERATIONAL SPECIFICATIONS</u>
<u>MODEL POPULATION</u>

in WAR UT2 2/day at LOC 29

in PEACE UT2 2/day at LOC 29

MOBILIZATION

in PEACE UT30 Messaging LOC 18 to LOC 19 UT5 for IMMEDIATE UPDATE



CONVERSION MAPPING MODEL POPULATION

User Task UT1 maps to
Program 1
Program 22

Idea Type ID1 maps to
Progm 1 dataelmnt 22
Progm 2 dataelmnt 28

Fig. 7. CFSSU Data Conversion Model

FILE # BP93050-3

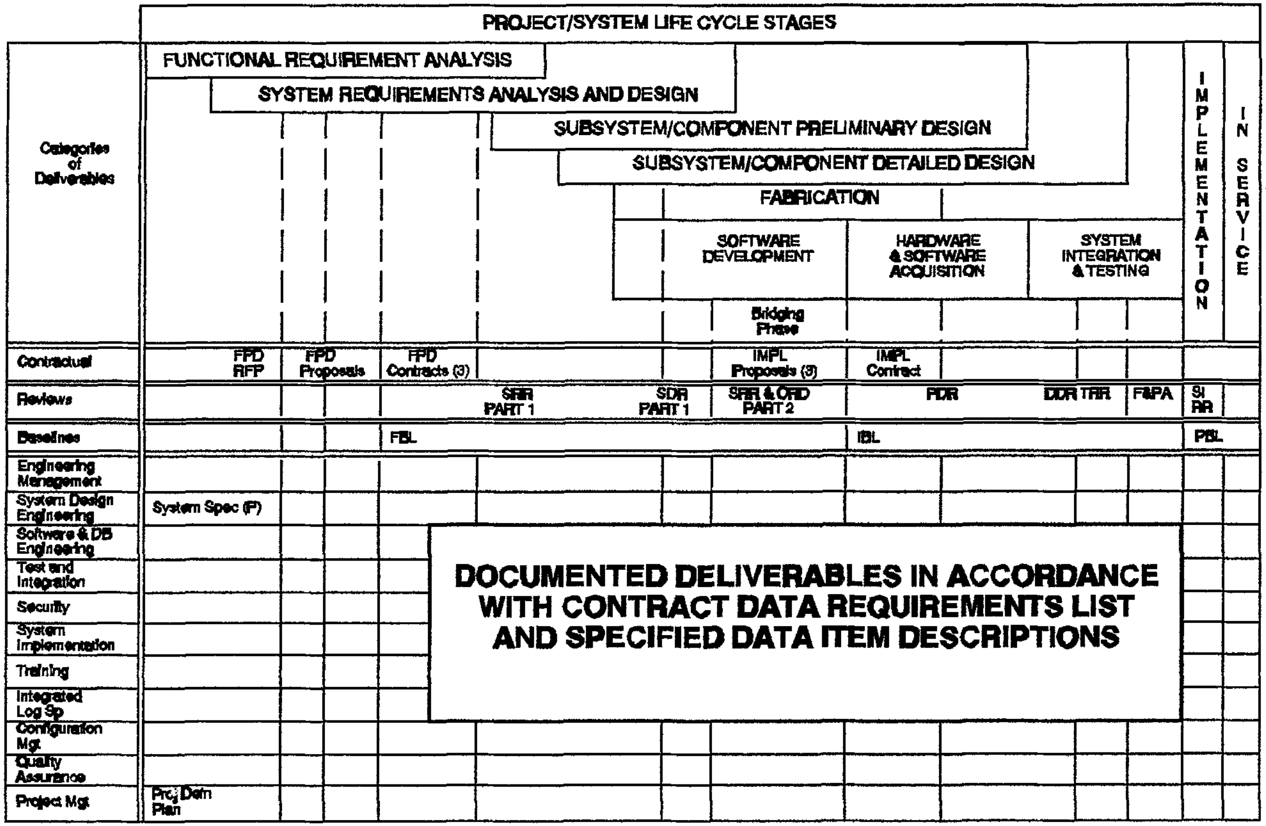


Fig. 8. CFSSU System Development Control Framework (Deliverables Chart) File # BP93055-3

References

1. ISO Technical Report TR 9007: Concepts and Terminology for the Conceptual Schema and the Information Base. International Organization for Standardization, Geneva.

2. Verheijen, G.M.A., and Van Bekkum, J.: NIAM, An Information Analysis Method. CRIS Report 1982, edited by T.W. Olle et al., Proceedings of the IFIP 8.1 Conference, North Holland.

3. Briefing to Industry, Canadian Forces Supply System Upgrade Project, Department of National Defence, Ottawa, Canada, 29 November 1989.

4. Briefing to Industry, Canadian Forces Supply System Upgrade Project, Department of National Defence, Ottawa, Canada, 22 June 1990.

5. Information Analysis Support Tools Reference Manual, Control Data Corporation, Minneapolis, USA, 1982, Revised 1983, 1985.