Proceedings of the Korean Nuclear Society Spring Meeting
Seoul, Korea, May 1998

Development of Requirements Tracking and Verification System for the Software Design of Distributed Control System

Chul Hwan Jung, Jang Yeol Kim, Jung Tack Kim, Jang Soo Lee and Chang Shik Ham

Korea Atomic Energy Research Institute
Man Machine Interface System Team
150 Dukjin-dong, Yusong-gu
Taejon, Korea 305-353

Abstract

In this paper a prototype of Requirement Tracking and Verification System(RTVS) for a Distributed Control System was implemented and tested. The RTVS is a software design and verification tool. The main functions required by the RTVS are managing, tracking and verification of the software requirements listed in the documentation of the DCS. The analysis of DCS software design procedures and interfaces with documents were performed to define the user of the RTVS, and the design requirements for RTVS were developed.

I. Introduction

The need for good requirements engineering and the consequences of a lack of it are most apparent in systems that are all or mostly software. It was observed from software requirements engineering that the value of good requirements and the criticality of doing them well increased dramatically with the size and complexity of the system being developed. Additionally, software-intensive systems seemed to have a more inherent complexity than systems that did not contain a great deal of software; thus these systems were more sensitive to the quality of their requirements. Requirements engineering is a part of system engineering. Requirement engineering practices are methodologies, methods, and tools of software requirements. The fundamentals of requirement engineering are decomposition and abstraction, allocation, flowdown, and traceability[1]. For a large-scale system development project to be successful, we must create flexible requirements management tool that can be adapted to fit a particular application environment. In the military industrial field a requirement management tool was developed and applied to their projects[2].

An advanced control system for a nuclear power plant is being designed using distributed control system(DCS). The progress of technology of computers and communications encourage the design method of instrumentation and control system of a nuclear power plant to adopt the advantages of digital technology. The role of software in the digital control system is more increased than in an analog control system and it is a very important point to the performance of control systems and the availability of a power plant.

To design the DCS software, the software requirement specification(SRS) which come from the program functional specification(PFS) is needed. Software engineers design the detail software with SRS. For software verification and testing the designed software is checked and compared with SRS. So a tool is needed to manage the requirements from the generation of requirements to the software validation stage.

In this paper and the prototype of the Requirements Tracking and Verification System (RTVS) for DCS design was implemented and tested, The analysis of DCS software design procedures and interfaces with documents of the CANDU 9 design were performed to define the user of RTVS, and the design requirements for RTVS were developed.

II. Software Design Procedures and Requirements

The RTVS shall be used during all the stages of software design, starting with the Program Functional Specifications and Device Control Requirements(DCR), and ending with the software validation stage. Figure 1 shows the users of RTVS based on the DCS software development scheme. This figure also shows the relationship between users and design documents.

The requirements for the DCS software will be derived from the Design Input Documentation(DID). The requirements stated in the PFS /DCR documents shall include application requirements derived from the plant system Design Descriptions (DD) and hardware related requirements derived from the DCS DD and sources applicable. The outputs of this requirements definition activity are the Software Requirement Specifications that present a formal statement of the DID requirements as they apply to the DCS application software.

During the definition of software requirements, software requirements will be allocated to partitions based on partitioning requirements contained in the DID and the Control System Application Design Guide(DG). The software designers enter the requirements stated in the DID and SRS into the RTVS database, in which traceability to the source of the requirement, and allocation to a given partition will be recorded. The software designer shall use the RTVS to verify that all the DID requirement have been mapped to SRS requirements and generate a cross reference report.

During the Software Requirements Review (SRR), the RTVS database shall be used as an aid in the review process as it provides a mapping of the DID requirements to the software requirements defined in the SRS. In the software design stage, SRS requirements will be allocated to Group and Device Control processors within each partition. Some requirements may be implemented partially at the Group Control Level, and partially at the Device Control level, resulting in the introduction of derived requirements allocated to each level. These derived requirements will be entered in the RTVS database, where their traceability to the parent requirement will also be recorded. Thus during software design stage, the RTVS will be used by software designers to show the derivation of requirements into new requirements, and how software requirements are addressed in the software design.

During the software design process, any need for a change to the requirements stated in SRS will be handled through the Software Change Request procedure. The RTVS will be used to assess the impact of the change and identify affected area(s) in detail before the change is approved.

III. Design requirements for RTVS

The design requirements for RTVS were developed and thir major requirements are listed in this section.

3.1 Data Recording Requirements

3.1.1 Data Input Requirements

a) The TRVS shall have the capability to record the information for each requirement entered in the RTVS database application.

b) The RTVS application should allow the data types to be assigned to information related with requirements of DCS.

c) The RTVS shall provide the data entry forms to the users for the data entering.

d) The RTVS application shall apply data type checking and data "masks" as appropriate to the input data to promote consistency within the RTVS database.

e) The RTVS shall incorporate data integrity functions to prevent inadvertent or unintentional operations from compromising or corrupting the RTVS database. User permission and data checking functions shall be provided to maintain strong data integration.

3.1.2 Requirement ID System Requirements

a) The RTVS shall ensure that all requirement identifiers are unique. The format of the identifier shall provide unique identifiers to be assigned to all DCS requirements and be composed of several alpha characters and digits, but the number of characters to make a unique requirement identifier shall not exceed 9 characters.

b) A status field shall be associated with each requirement. The status field shall be able to be assigned the following values:

i) Active: requirement is valid,

ii) Deleted: requirement is no longer valid,

iii) Superseded: requirement is no longer valid and has been replaced by another, and

In-progress: some information relating to the requirement is incomplete.

c) The RTVS shall be capable of managing different versions of the requirements but shall not allow more than one version to be assigned a status value of active.

d) The RTVS application shall be capable of managing statement of requirements which are represented in graphical or tabular format where practical. Where this is not practical, these requirements may be assigned a requirement ID that will be entered in the RTVS database and cross referenced to the original definition.

3.2 Display Requirements

a) The RTVS shall provide the user interface displays to enter data and to control the management functions.

b) The RTVS shall provide the data entry display for the software Designer, Verifier and Reviewer. Each data entry display shall contain the form which is defined by 3.1.1c).

3.3 Data Management Requirements

a) The RTVS shall provide the management functions to manage the data of the requirements and the information related with requirements of DCS.

The management functions shall consist of:

i) TRACEABILITY: allows the user to displays the relationship between requirements,

ii) DERIVE : allows the user to generate new derived requirements,

iii) SUPERSEDE: allows the user to generate a new requirement or define an existing requirement that supersedes an existing requirement,

iv) EDIT/CREATE: allows the user to select and edit an existing requirement or create a new requirement,

v) SAVE: saves the current on-screen version of the requirement,

vi) DELETE: changes the status of the requirement to deleted,

vii) PURGE: deletes the data associated with a requirement with a "deleted" status from the RTVS database,

viii) SEARCH: allows the user to view and/or sort data from the RTVS database based on user defined query information,

ix) REPORT: allows the user to output the results of a search to a printing device or file,

x) HELP/ERROR CODES: provides the user with context sensitive help and error messages,

xi) COMPLIANCE: allows the requirement reviewer (as part of either the SRR or SDR) to indicate compliance of the requirement with its source. For a requirement reviewer the fields of PASS REVIEW and FAIL REVIEW are required. For a software design reviewer the fields of COMPLY and DO NOT COMPLY are required,

xii) TEST DATA: allows users to enter data regarding software tests (defining applicable test cases and their results), and

xiii) ADMIN: allows the RTVS administrator to define user permissions.

b) The RTVS shall have the ability to define and manage hierarchical relationships between requirements and differentiate between relationships where both requirements are in the same document and those where the two requirements are in separate documents.

c) The RTVS shall trace the ancestor and descendant of a requirement and shall trace the origin also.

d) The RTVS shall have the ability to define a relationship where a new (or existing) requirement is identified as being derived from the requirements of another and represent this relationship in a hierarchical structure.

e) The RTVS shall provide means for the verification and validation (V & V) activities to state their conclusions such as Pass, Fail, Comply etc. Each of the V & V related fields shall be identified individually with reference to the V & V report name and number. For a software tester the fields of the PASS and FAIL are required to store the result of comparison between a requirement and a designed software function. The RTVS shall provide a method for the reviewer to acknowledge the results of their review activity. For a requirements reviewer, the fields of PASS REVIEW and FAIL REVIEW shall be available. For a software reviewer the fields of COMPLY and DO NOT COMPLY shall be available..

f) The RTVS shall provide means of superseding of the requirements.

g) If a new requirement supersedes a requirement, a new requirement should inherit the relationship from the old requirement or RTVS should have means to define new relationship of a new requirement and to delete the relationship of a superseded (old) requirement

h) It shall be easy to add, change, and manipulate the requirements and requirements related information of DCS. A menu driven method shall be adopted for this purpose.

i) The RTVS shall provide RTVS functions according to the permissions granted to the user which shall be established by assigning the user to a pre-defined user type.

3.4 Report Requirements

a) The RTVS shall provide several report formats to the user. The report formats shall include detailed requirement report formats, the DCS requirement documentation type formats, and requirement tree report formats. The RTVS shall have a report design function to allow the user to produce custom reports.

b) From the requirement tree reports, the user should be able to easily establish the relationships between requirements.

c) It shall be possible to view the RTVS reports on the workstation display, save them to an ASCII file, or print them on a printer user menu driven commands.

3.5 Performance Requirements

a) The RTVS shall have data storage space and processing capability for the processing data for of nearly 50,000 unique requirements (including antecedents).

b) For routine operations, the user should not experience more than a 10 second wait for the RTVS application to display the results of a user data query function.

c) All routine data management functions should provide the processing results to the user with a response time of less than 10 seconds.

3.6 Maintainability Requirements

a) RTVS shall be designed with administrative controls in place to prevent unauthorised changes being made to either the configuration of the RTVS or the application data held within database(s) generated by the RTVS.

b) The design of the RTVS shall not limit the ability to expand its functionality in the future nor take advantage of subsequent upgrades to its development platform or RDBMS.

IV. The development of prototype RTVS

For the development of design requirements and a prototype of RTVS, the liquid zone control(LZC) system of CANDU 9 DCS was selected as a sample system. The related documents to the LZC design, the PFS[3] and SRS[4], were used. The MS Access was used as relational RTVS database. For the generation of sample data we analysed the relationship of requirements and documents, and set the levels of sample requirements and the requirement ID pattern. Figure 2 shows a display of requirement data entering and figure 3 shows a trace display of

a requirement. After the application test of RTVS, the requirements which were not established, nor implemented at the time that the prototype application was developed were added to the design requirement of RTVS.

V. Conclusion

In this paper a prototype of Requirement Tracking and Verification System(RTVS), a software design and verification tool, for a Distributed Control System was implemented and tested. The analysis of DCS software design procedures and interfaces with documents were performed to define the user of the RTVS, and the design requirements for RTVS was developed. The main functions of the RTVS are managing, tracking and verification of the software requirements listed in the documentation of the DCS. An advanced control system for a nuclear power plant is being designed using a distributed control system. The role of software in the digital control system is a very important point to the performance of control systems and the availability of a power plant. So we should develop the related technology of the RTVS to have high quality DCS software design technology, and to save the DCS cost of software.

VI. References

[1] M. Dorfman, System and Software Requirements Engineering, EH0304-6/90/0000/0004, pp. 4-15, 1990 IEEE.

[2] R. F. Flynn and M. Dorfman, The automated requirements traceability system: An experience of eight years, EH0304-6/90/0000/0423, pp. 423-437, 1990 IEEE.

[3] 69-63720-PFS-001, Rev. 0, Program Functional Specification, Liquid Zone Reactivity Control.

[4] 69-63720-SRS-001, Rev. 0, Software Requirement Specification, Sample SRS-Liquid Zone Reactivity Control.

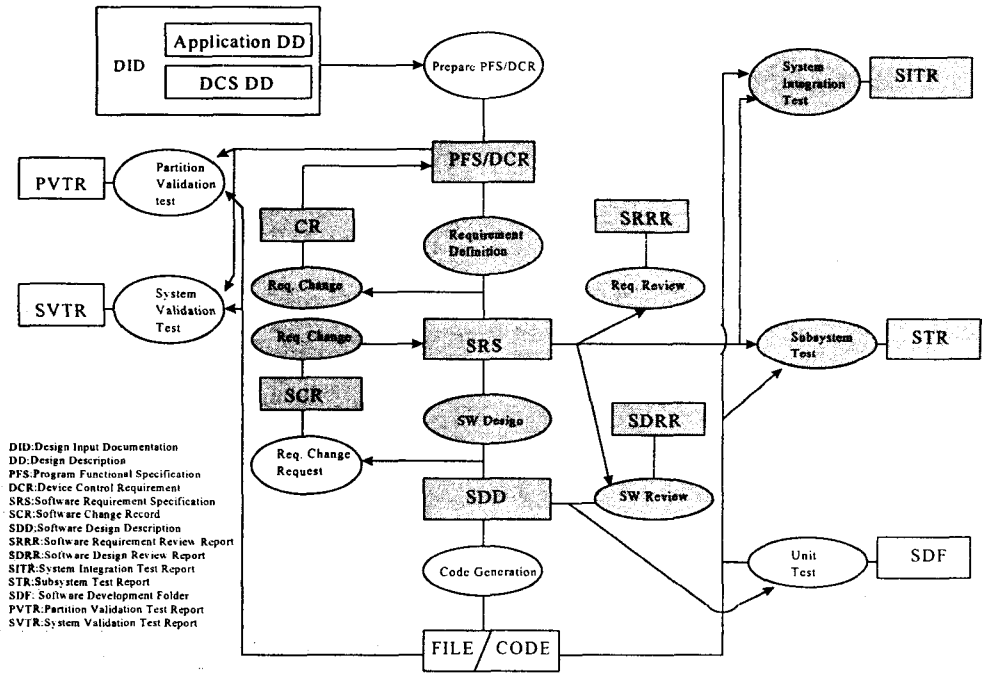

Figure 1. Users of the RTVS

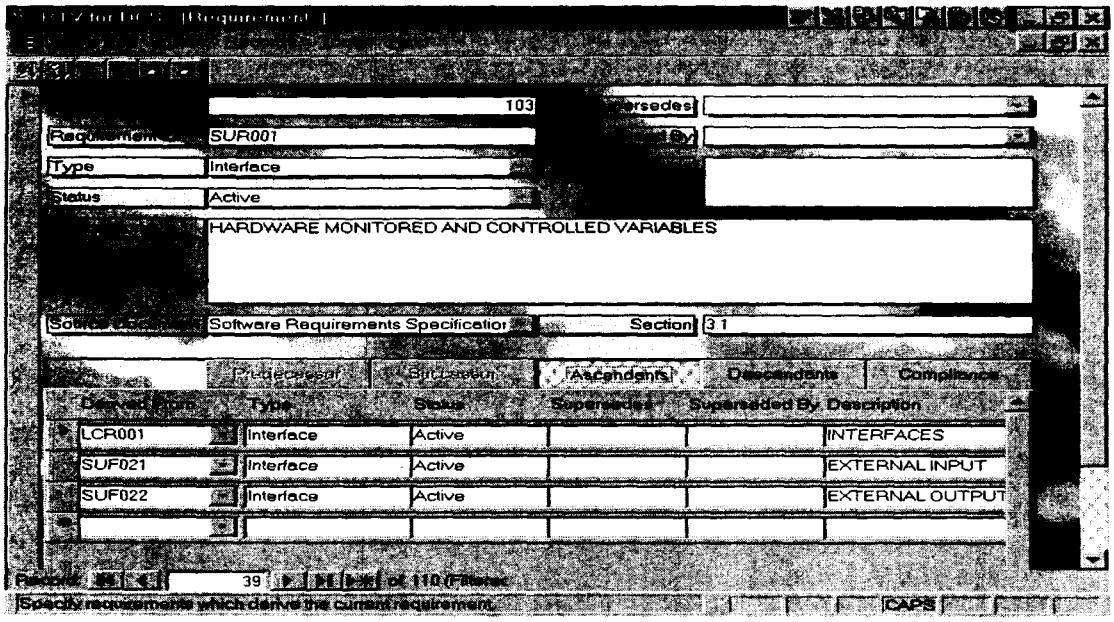

Figure 2. A display of RTVS for data recording of requirement

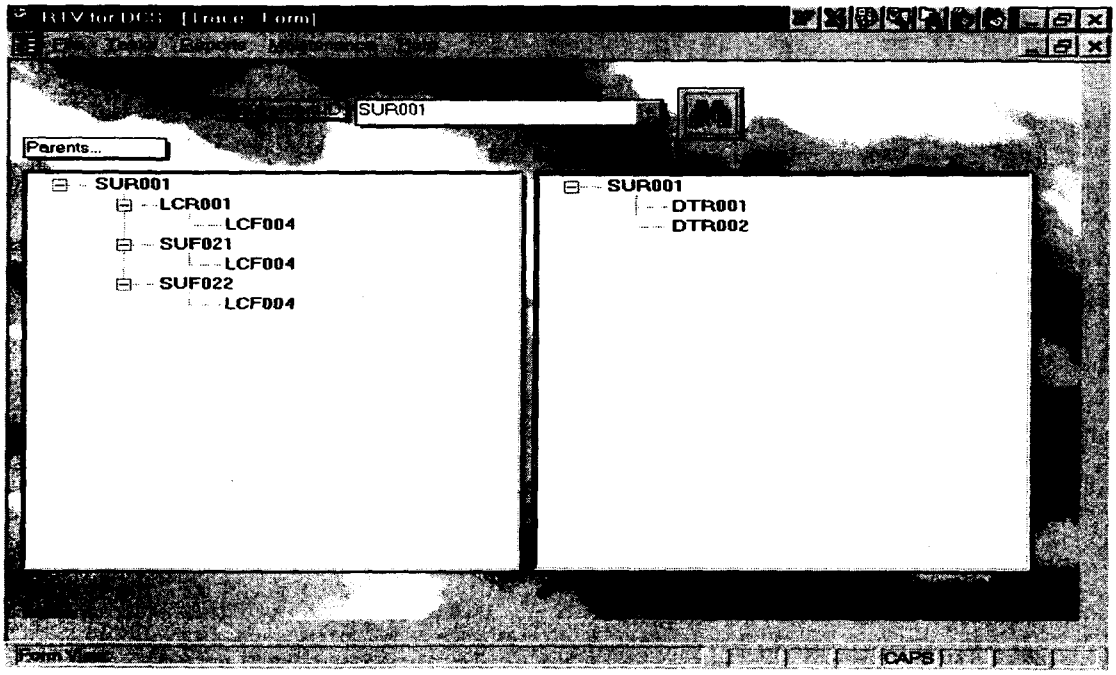

Figure 3. A trace display of a requirement