Pacific Northwest National Laboratory
Operated by Battelle for the
U.S. Department of Energy

FRAMES-2.0 Software System: Providing Password Protection and Limited Access to Models and Simulations

G. Whelan
M. A. Pelton

August 2007

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, makes **any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights**. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576 5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service,
U.S. Department of Commerce, 5285 Port Royal Rd., Springfield, VA 22161
ph: (800) 553-6847
fax: (703) 605-6900
email: orders@nits.fedworld.gov
online ordering: http://www.ntis.gov/ordering.htm

FRAMES-2.0 Software System: Providing Password Protection and Limited Access to Models and Simulations

G. Whelan
M. A. Pelton

August 2007

Summary

Regulatory agencies use the concept of reproducibility to provide added credibility to assessments. The use of well-documented and -tested assessment models is an important aspect of confirming reproducibility. The U.S. Nuclear Regulatory Commission (NRC) provides guidance for appropriate approaches, assessment models, and databases to help meet regulatory requirements. Because multiple groups are engaged in environmental and safety assessments for a wide variety of sites, this approach provides a consistent basis for assessments. The objective of this effort is to provide NRC with a means to restrict access to a suggested set of models, databases, and conceptual site models (CSMs) (i.e., picture-containing linked icons), where appropriate, using the Framework for Risk Analysis in Multimedia Environmental Systems (FRAMES)-2.0 software system. The purpose is to provide an ability to "lock down" the CSM, restrict access to certain models, or both. Three locking options have been developed, tested, and documented:

1. Models Associated with a Domain—lock the number of models allowed within the Domain,[a] which includes the set of dictionaries. Locking down models means that models affiliated with the Domains cannot be removed or added without a password.

2. CSM Simulation—lock the CSM simulation picture. Altering icons and the way in which they are connected to each other will not be allowed. The icons are fixed and so are their connections.

3. Model associated with an Icon Type—lock a specific model to a specific icon type (e.g., Reactive Multi-Species Transport in Three-Dimension [RT3D] module to an Aquifer icon). Only one applicable model will be available to the user, assuming the connections are valid.

These modifications to FRAMES allow multiple groups to work on similar problems without inadvertently changing the CSM and/or the models available to the user in the assessment. This will help confirm that the problems being modeled (i.e., CSM), and the models and databases that represent the components are consistent, allowing for reproducible results regardless of the host computer or user.

Section 1 provides an introduction that explains the objective of this task, three locking options, and two ways to implement the desired locking features. Section 2 discusses locking-mechanism requirements for models associated with a domain, CSMs, and models associated with an icon type. Section 3 discusses the design elements for models associated with a Domain, CSM simulation, and models associated with an icon type. Issues regarding specifications are explained (Section 4) as well as the testing approach and results (Section 5).

(a) In context of FRAMES, a Domain represents a specific collection of models, usually created by a user for a special purpose (e.g., 3MRA Domain).

Acronyms and Abbreviations

3MRA	Multi-media, Multi-pathway, Multi-exposure Risk Assessment
CRC	cyclic redundancy check
CSM	Conceptual Site Model, simplified description of the environmental problem to be modeled
DCE	Data Client Editor
DLL	dynamic link library
DOE	U.S. Department of Energy
EPA	U.S. Environmental Protection Agency
FDE	Framework Development Environment
FRAMES	Framework for Risk Analysis in Multimedia Environmental Systems
GMS	Groundwater Modeling System
HWIR	Hazardous-Waste Identification Rule
MT3DMS	Modular Three-Dimensional Multi-Species Transport Model
NRC	U.S. Nuclear Regulatory Commission
PNNL	Pacific Northwest National Laboratory
QA/QC	quality assurance/quality control
RT3D	Reactive Multi-Species Transport in Three-Dimension (module)

Acknowledgments

Contents

Figures

Tables

1.0   Introduction

Reproducibility in regulatory assessments represents an important component of the quality assurance/quality control (QA/QC) process, as reproducibility provides an important component of credibility. The U.S. Nuclear Regulatory Commission (NRC) provides guidance for appropriate approaches, assessment models, and databases to help meet regulatory requirements. Because multiple groups are engaged in environmental and safety assessments for a wide variety of sites, this approach provides a consistent basis for assessments.

Reproducibility was a key requirement when the U.S. Environmental Protection Agency (EPA) developed and implemented the Multi-media, Multi-pathway, Multi-exposure Risk Assessment (3MRA) methodology (http://www.epa.gov/ceampubl/mmedia/3mra/index.htm), as applied to the Hazardous Waste Identification Rule (HWIR). Seventeen different models, five different databases, and five different processors were combined to address the needs of HWIR (http://www.epa.gov/epaoswer/hazwaste/id/hwirmdia.htm). Because multiple groups were working on the same problem and because this system was to be distributed to anyone who requested it, regulatory protocol required that the assessment situations and models comprising the assessment were locked to confirm that everyone was solving the same problems and using the same analysis codes.

The objective of this effort is to provide a similar capability to NRC through the Framework for Risk Analysis in Multimedia Environmental Systems (FRAMES) modeling platform. A mechanism is provided to limit user access to a suggested set of models and databases, and constrain the CSM (i.e., picture-containing linked icons) where appropriate. The purpose is to provide the ability to "lock down" the CSM (i.e., picture-containing linked icons), restrict access to certain models, or both. Three locking options are summarized as follows:

1. Models Associated with a Domain—lock the number of models allowed within the Domains, which includes the set of dictionaries. Locking down models means that models that are affiliated with the Domains cannot be removed or added without a password.

2. CSM Simulation—lock the CSM simulation picture. The icons and the way in which they are connected to each other will not be allowed to be altered. The icons are fixed and so are their connections.

3. Model Associated with an Icon Type—lock a specific model to a specific icon type (e.g., single groundwater model to an Aquifer icon). Only one applicable model will be available to the user, assuming the connections are valid.

Because there are two choices (i.e., lock or unlock) with each option, eight permutations exist (i.e., $2\times2\times2$). There are two ways of implementing the desired locking features:

1. Client Side—Locking/unlocking on the client side can be implemented in the FRAMES-2.0 user interface, called the Framework Development Environment (FDE). This can be achieved with password-protection without modifying the dynamic link library (DLL). Because the FDE is not locked at the server level, it is susceptible to subversion.

2. Server Side—Locking/unlocking on the client side is more involved and would require more effort, but confirms that virtually no one could subvert the system. This option would be ideal if the Framework for Risk Analysis in Multimedia Environmental Systems (FRAMES) was web-based.

Modifications to the client side (i.e., Option 1) will be implemented because as FRAMES migrates to being a server-side software product, server-side modifications made today may become obsolete in the future.

In summary, three password-protected locking options will be implemented at three levels in the FRAMES hierarchy: Domain level, CSM level, and icon-type level. For the Domain level, the password is not user-defined but a function of the computer to which FRAMES is installed and the time it is installed. A password generator is, therefore, required to provide an independent, reproducible, and verifiable password, which is machine and time dependent. The passwords associated with the CSM and icon type are user-defined.

2.0 Requirements

Requirements are characteristics and behaviors that a piece of software must possess to function adequately for its intended purpose. Password protection and limited access to models and simulations represent fundamental capabilities in FRAMES to support regulatory QA/QC protocols. The following requirements pertain to the client-side option.

2.1 Models Associated with a Domain

The current version of FRAMES-2.0 allows for the user to create separate Domains and limit the number and types of models associated with each Domain. These modifications shall

1. be visible as a choice (e.g., Lock or Unlock) within the File menu in the main FDE screen when outside of the editors (e.g., [Units] Conversion, Dictionary, Module, Domain, and Simulation).

2. allow the user, within a menu option, to "lock" the Domain when it is in an unlocked state.

3. allow the user, within a menu option, to "unlock" the Domain when it is in a locked state.

4. open to the Simulation Editor (i.e., CSM screen) with a locked Domain.

5. contain a symbol in the FDE indicating the locked or unlocked state of the Domain.

6. retain the locked or unlocked state when the simulation is saved, copied, or packaged and unpackaged using the Simulation Packager and Simulation Unpackager, respectively.

7. confirm that the password is machine and time (i.e., at the time of the install) dependent, not user-defined.

8. provide a mechanism to determine an independent password (e.g., Password Generator).

9. close by asking the user if he/she would like to save any changes.

10. allow the user to view the contents of the Dictionary, Module, Domain, and (Units) Conversion Editors, but do not allow the user to make modifications when locked.

2.2 Conceptual Site Model Simulation

Under this option, modifications will lock the CSM simulation picture and provide password protection from subverting the icon choices and connection schemes. These modifications shall

1. be visible as a choice within the File menu when in the Simulation Editor

2. only lock/unlock the current simulation

3. allow the user, within the File menu, to "lock" a simulation when it is in an unlocked state

4. allow the user, within the File menu, to "unlock" a simulation when it is in a locked state

5. prompt the user for a password when unlocking

6. prompt the user for a password and duplicate the password when locking

7. contain a symbol in the Simulation Editor, indicating the locked or unlocked state of the CSM

8. retain the locked or unlocked state when the simulation is saved, copied, or packaged and unpackaged using the Simulation Packager and Simulation Unpackager, respectively

9. close by asking the user if he/she would like to save any changes.

2.3 Model Associated with an Icon Type

Under this option, modifications will lock in a specific model to a specific icon type (e.g., Reactive Multi-Species Transport in Three-Dimension [RT3D] module to the Aquifer icon) and provide password protection from subverting the model choice. These modifications shall

1. be visible as an option within the icon user interface (i.e., right-click on icon)

2. only lock/unlock the current selected icon

3. allow the user, within the icon user interface, to "lock" a model when it is in an unlocked state

4. allow the user, within the icon user interface, to "unlock" a model when it is in a locked state

5. not allow the user access to other applicable model choices when locked

6. retain the locked or unlocked state when the simulation is saved, copied, or packaged and unpackaged using the Simulation Packager and Simulation Unpackager, respectively

7. prompt the user for a password when unlocking

8. prompt the user for a password and duplicate the password when locking

9. provide a visual icon overlay indicating the lock status on the module icon

10. close by asking the user if he/she would like to save any changes

11. confirm that a model has been selected before allowing for it to be locked.

3.0 Design

Design elements are strategies for meeting requirements. The requirements will be implemented with the concept that when a model or simulation is locked, the locking mechanism will be maintained even if the simulation is saved (e.g., "Saved As"), copied, or packaged, and no effort will be made to remove the locking mechanism. If the correct version of FRAMES (i.e., Lock/Unlock version) is not used, then a locked version of the simulation will not work because of dictionary differences. In other words, once the locking mechanism is turned on in the new version of FRAMES, it will not be backward compatible with previously developed simulations. Client-side modifications will be implemented to meet the needs of locking models and simulations associated with FRAMES. The FDE is the only piece of software that will change. Three locking options are summarized as follows: 1) models associated with a Domain, 2) CSM simulation, and 3) model associated with an icon type.

3.1 Models Associated with a Domain: Limiting the Number of Models Allowed Within a Domain

Users will have the ability to develop their own Domains, containing only those models they so desire. When new Domains are created, the user will still have the ability to include new models through the registration process (i.e., Module, Dictionary, Domain, and (Units) Conversion Editors). Once registered to a new Domain, only those registered models will appear in the model listings under each icon. The choice of models for the Domain is limited to only those models registered in the Domain. Different Domains can have different models registered to them. The Domains, which are defined in the system, can be viewed by going to the FDE user interface, "Editors" menu, "Simulation Editor." Figure 3.1 illustrates three Domains: Environmental Domain, 3MRA Domain, and System Domain.

3.1.1 Unlocking Domains

From the moment the user enters the FDE, the Domain is locked. The first screen encountered by the user, under the Simulation Editor, is the Environmental Domain with the CSM user interface, containing the global and local work spaces, as illustrated by Figure 3.2. Figure 3.2 shows that the Domains are locked, as a picture of a padlock appears in the upper left-hand corner of the CSM user interface. This figure also signifies that the CSM is unlocked as the FRAMES symbol appears immediately below the padlock. To unlock the Domain, use the following steps:

1. The user first needs to Exit the Simulation Editor (go to File menu, and choose Exit). The screen will return to the FDE user interface, as illustrated by Figure 3.3a. Note that the FDE user interface signifies that the Domains are locked by displaying a padlock in the upper left-hand corner, as illustrated in Figure 3.3a.

2. To allow the user to add or remove models to or from Domains, respectively, go the File menu and choose "Unlock System" as illustrated in Figure 3.3a.

3. The user will be asked to supply the password to unlock the Domains, as illustrated in Figure 3.4. To obtain a password, the user will need to contact the appropriate personnel who have a copy of the Password Generator. The Password Generator supplies a machine- and time-dependent password. A description of the Password Generator is provided in a succeeding section, titled Password Generator.
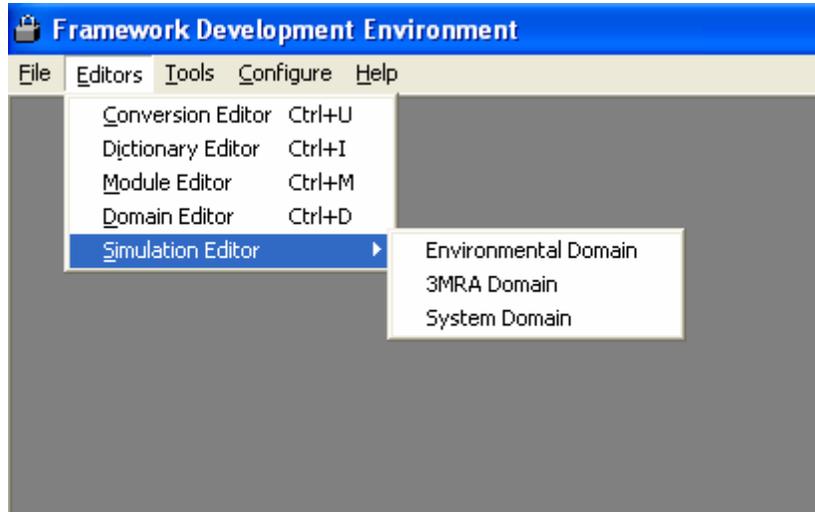
Figure 3.1. Domains Currently Defined Within FRAMES: Environmental Domain, 3MRA Domain, and System Domain

Figure 3.2. CSM User Interface, Containing the Global and Local Work Spaces, Showing that the Domains Are Locked (depicted by a padlock) and CSM Is Unlocked (depicted by a FRAMES-2 picture, that is, no padlock)
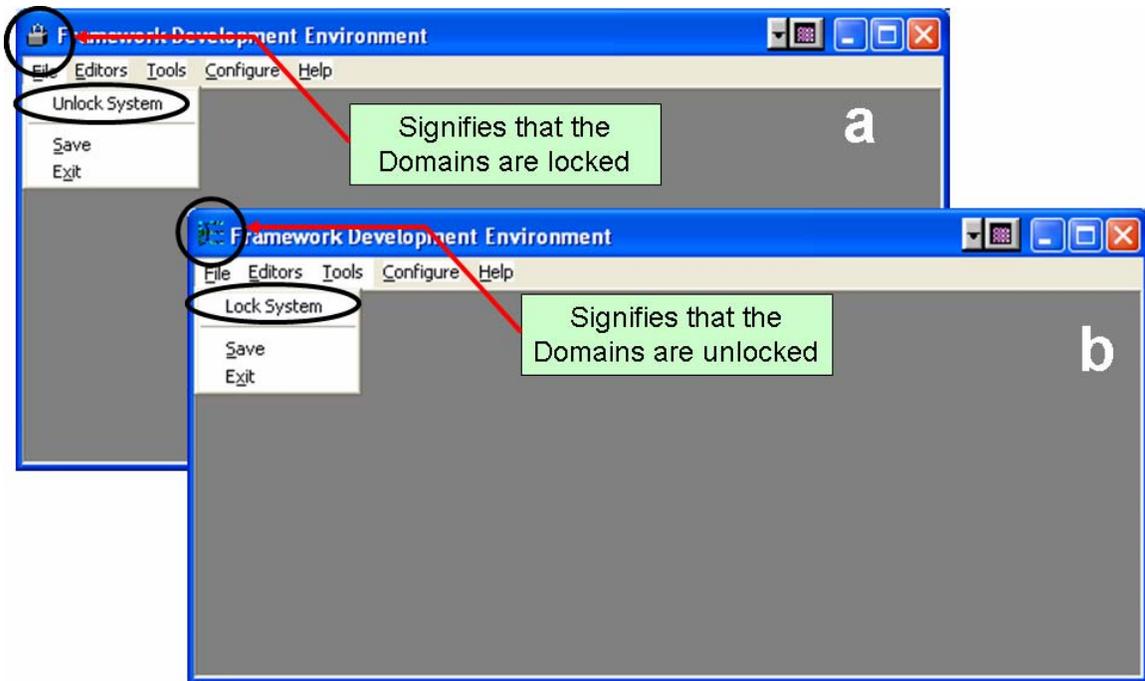
Figure 3.3. Screen Captures of the FDE User Interface, Showing the Location to Unlock (in "a") or lock (in "b") Domains in the File Menu Where the Padlock Signifies that the Domains Are Currently Locked, and the FRAMES-2 Icon (no padlock) Signifies that the Domains Are Currently Unlocked
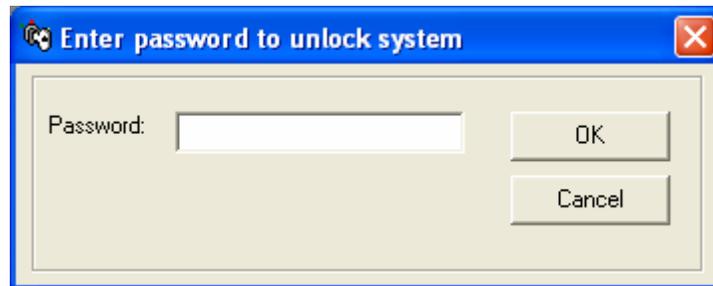
Figure 3.4. Screen Capture for a User to Enter a Password to Unlock the System when Domains Are Locked

3.1.2 Locking Domains

To lock the Domains, the user follows a similar procedure as that outlined when unlocking the domains:

1. The system signifies that the Domains are unlocked by not displaying a padlock in the upper left-hand corner of the FDE user interface, as illustrated in Figure 3.3b.

2. To lock the Domains, go the File menu and choose "Lock System" as illustrated in Figure 3.3b.

3. The user will not be asked to supply the password to lock the Domains because the password is not user-defined but uniquely defined by the system, based on the specific machine and the time the latest install occurred. The user can tell when the system becomes locked because the padlock will be displayed in the upper left-hand corner of the FDE user interface (Figure 3.2a).

When the domains are locked, the user locks the number of models allowed within a Domain, which includes the set of dictionaries. Locking down models means that models that are affiliated with the Domain cannot be removed or added without a password. Locking Domains does not prevent the user from viewing the attributes associated with the various editors associated with the system (i.e., [Units] Conversion, Dictionary, Module, and Domain). As Figure 3.5 illustrates, all of the attributes associated with the Module Editor are available to the user to view. These attributes are locked down though, and all functionality to use the Module Editor to change attributes is greyed out.
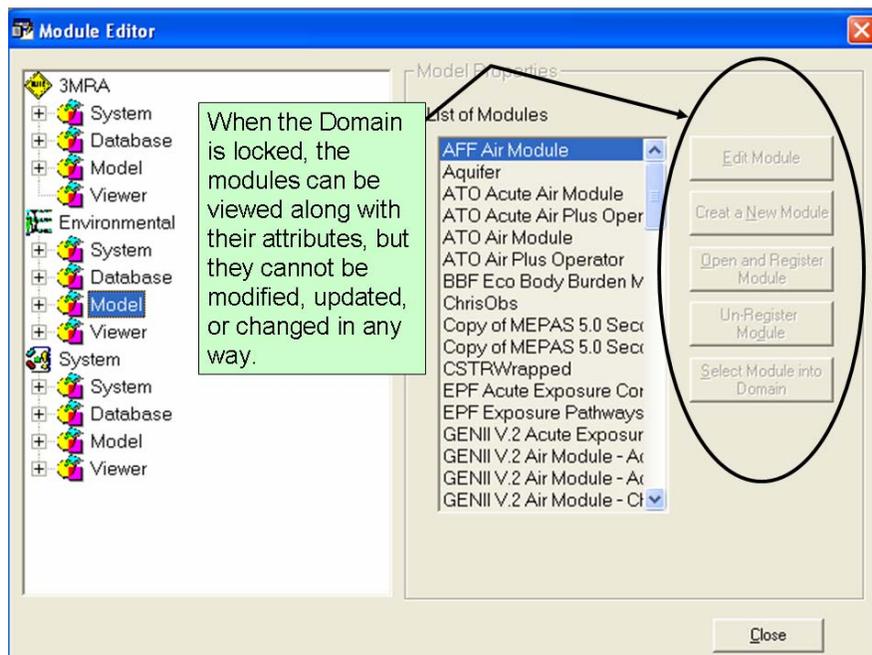
Figure 3.5. Screen Capture of a Module Editor User Interface when the Domains Are Locked; All Action Buttons Are Grayed Out

3.1.3 Password Generator

The Password Generator is a separate piece of software that allows users to limit which models are affiliated with their particular Domain. As noted in the Introduction, the 3MRA methodology, as applied to HWIR, contains 17 different models, 5 different databases, and 5 different processors. Because multiple groups were working on the same problem and because this system was to be distributed to anyone who requested it, regulatory protocol required that

the assessment situations and models comprising the assessment were locked to confirm that everyone was solving the same problems and reproducing the same results. Figure 3.1 shows that a separate 3MRA Domain has been created.

To unlock the Domain, the user requires a password. The unique password is machine specific and specific to the time when the last install occurred. A piece of software will generate this unique password and will be called the Password Generator. The Password Generator will generate an eight-character password from an integer between 1 and 20,000,000, use ASCII character codes that fall between 64 to 128 inclusive, and use the same algorithm used by FDE.exe in FRAMES to obtain the password. When the FRAMES software is installed on a specific machine, a unique number, called the "Installation CRC" number, is defined. CRC stands for cyclic redundancy check. The installation CRC number can be found under the "Help" menu, "About," as illustrated in Figure 3.6. The text box requesting the Installation CRC number only accepts numbers between 1 and 20,000,000 as input. The Password Generator will produce a unique identifier, which is displayed as **^Ak^sMa@** in Figure 3.6. The second text box is not editable but can be copied. An error message will be displayed when and if the "Generate password" button is pressed, and the value in the first text box is unacceptable, as illustrated in Figure 3.7.
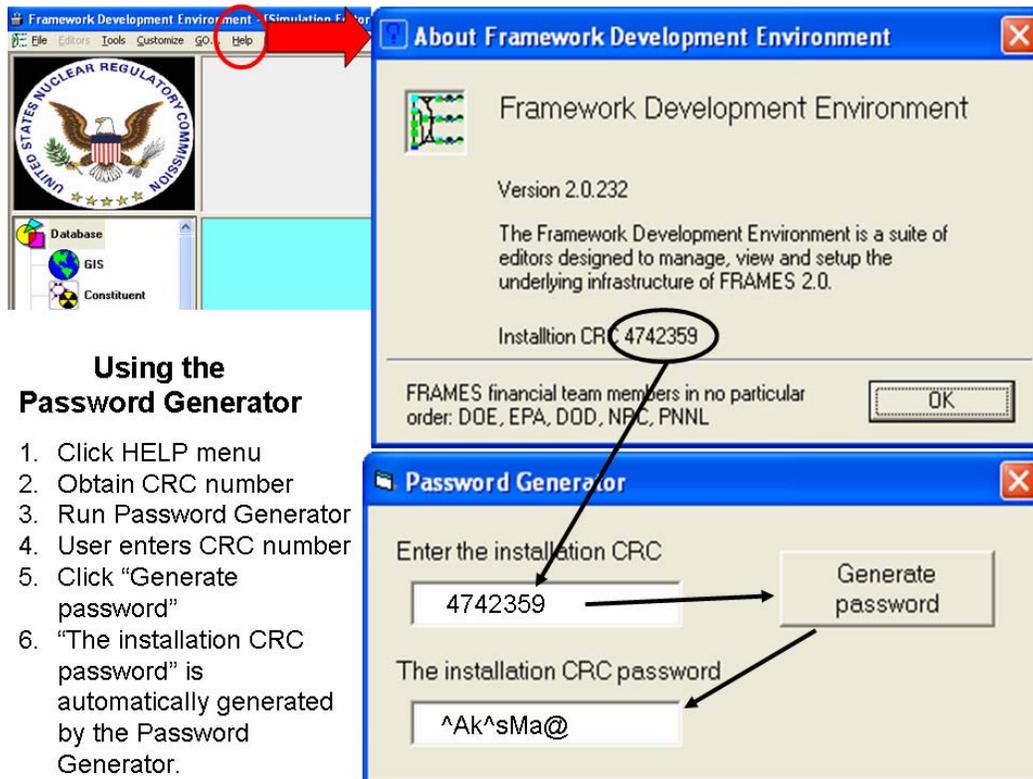
Figure 3.6. Procedure to Determine the Installation CRC Password Using the Password Generator
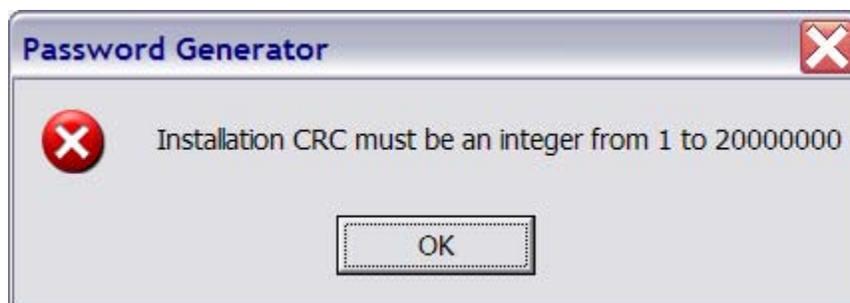
Figure 3.7. Error Message when the User Enters an Illegal Entry into the Password Generator

3.2 Conceptual Site Model Simulation: Lock the CSM Simulation Picture

Users will have the ability to develop CSMs, representing standard environmental situations that need to be evaluated, regardless of the location of the physical setting, although physical settings would be of the same genre. For example, Figure 3.8 could represent a standard and reusable CSM. This figure depicts user-defined, environmental-contaminant levels ("User-Defined") that impact the food chain before intake (Exposure Pathways), resulting in contamination that passes into the human body at a certain intake rate ("Receptor Intakes"), resulting in an impact ("Health Impacts"). To lock this CSM, as illustrated in Figure 3.8, the user goes to the File menu and chooses "Lock," as illustrated in Figure 3.9. A user interface will appear, like Figure 3.10, and the user is free to define a password to lock the CSM. When the user exits, the screen will convey to the user that the CSM is locked, and modifications to it will not be possible, like adding new icons or modifying connections. Under locked conditions, the screen will depict the picture of a padlock in the upper left hand corner of the CSM, as illustrated in Figure 3.8. Again, models under each icon may still be selected, but no new connections in the CSM picture will be allowed. Likewise, if the user wants to unlock the CSM (assuming that it is locked), the user again goes to the File menu and chooses "Unlock." The user will see either Lock or Unlock in the File menu, but not both.
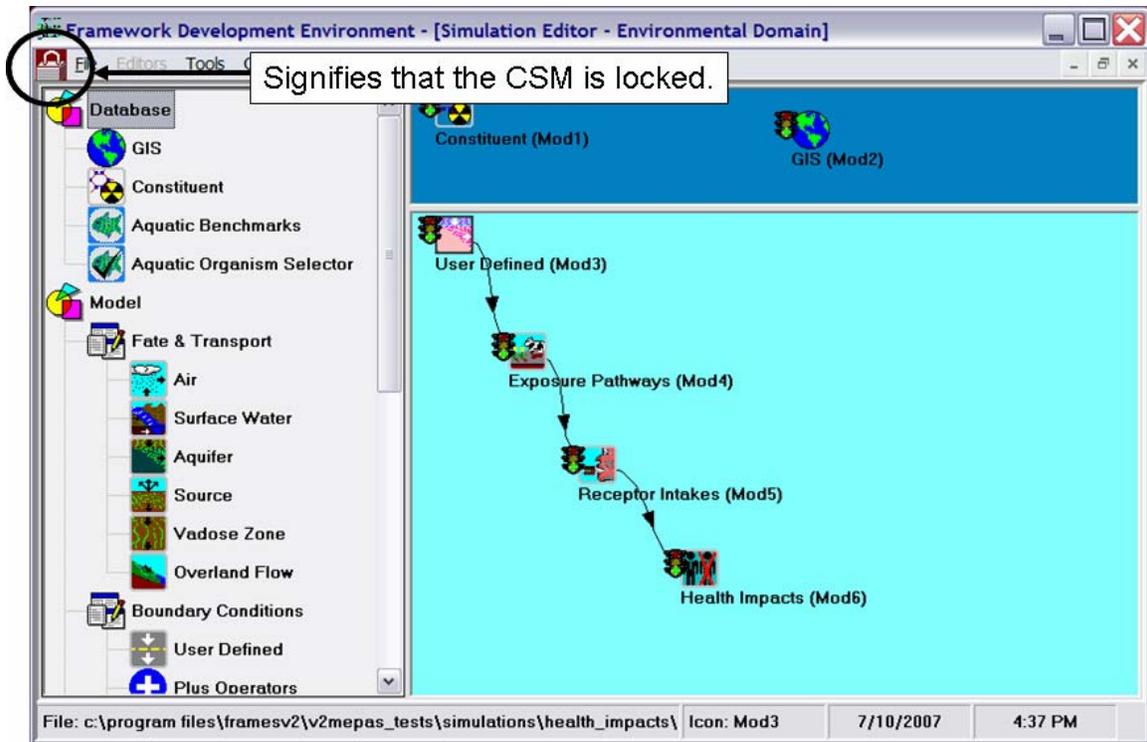
Figure 3.8. Screen Capture of the Simulation Editor CSM with the Picture of a Padlock, which signifies that the CSM Is Locked
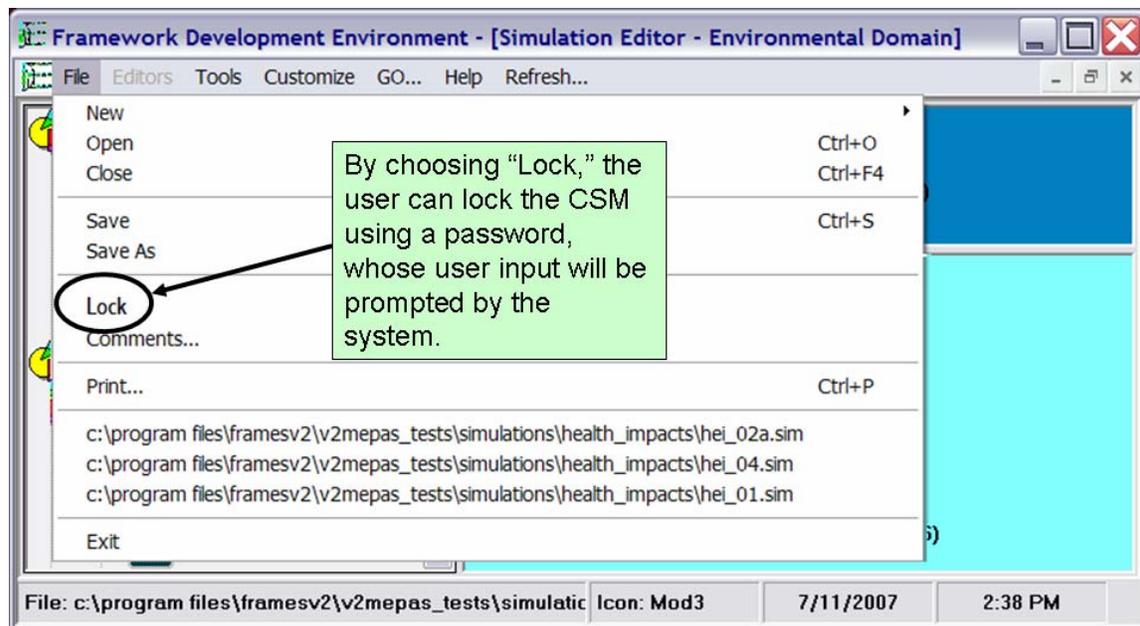
Figure 3.9. Screen Capture of the File Menu in the Simulation Editor Identifying the Location of the Procedure for Locking the CSM
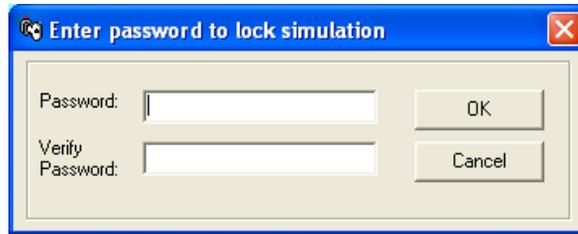
Figure 3.10. Screen Capture for a User to Enter a Password to Lock the CSM Simulation

3.3 Model Associated with an Icon Type: Lock in a Specific Model to a Specific Icon Type

Users will have the ability to assign one applicable model to represent an icon type and lock that model to that icon type (e.g., "Aquifer"). For example, if all aquifer modeling is to be performed using RT3D, then the user has the ability to limit the Aquifer icon to use only RT3D. This functionality will be available through the icon's user interface (i.e., right-hand click) as illustrated in Figure 3.11. Figure 3.11 illustrates a new menu option containing the "Lock" choice, for the Exposure Pathways (Mod4). When the user chooses "Lock," a user interface will appear, as depicted in Figure 3.12a, allowing the user to password protect the model choice. When the user exits the icon menu, the system modifies the icon picture by including a padlock, as illustrated in Figure 3.13. Once the model has been chosen and locked, "General Info" will be greyed out, as shown in Figure 3.14, not allowing the user to choose a different model. If the user wants to unlock the system, "Unlock" is chosen from the module user interface, and the user will be requested to supply the correct password, as illustrated in Figure 3.12b.
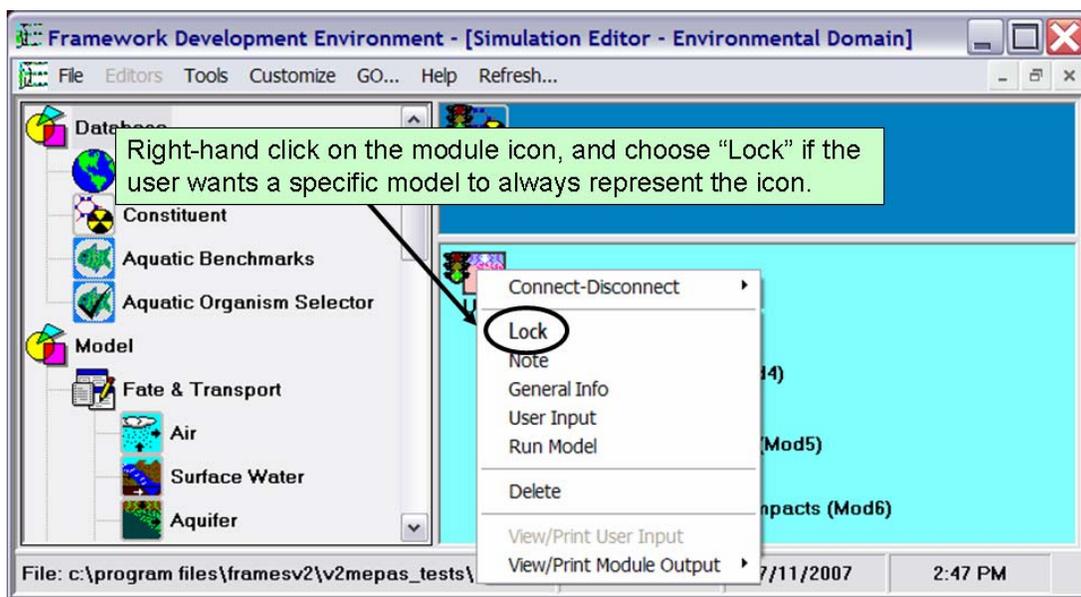
Figure 3.11. Screen Capture of the Right-Click Icon Menu Showing How the User Can Lock the Model Associated with an Icon Type

3.8

Figure 3.12. Screen Captures of the User Interfaces Requesting the User for a Password to (a) Lock and (b) Unlock the Model Associated with an Icon Type
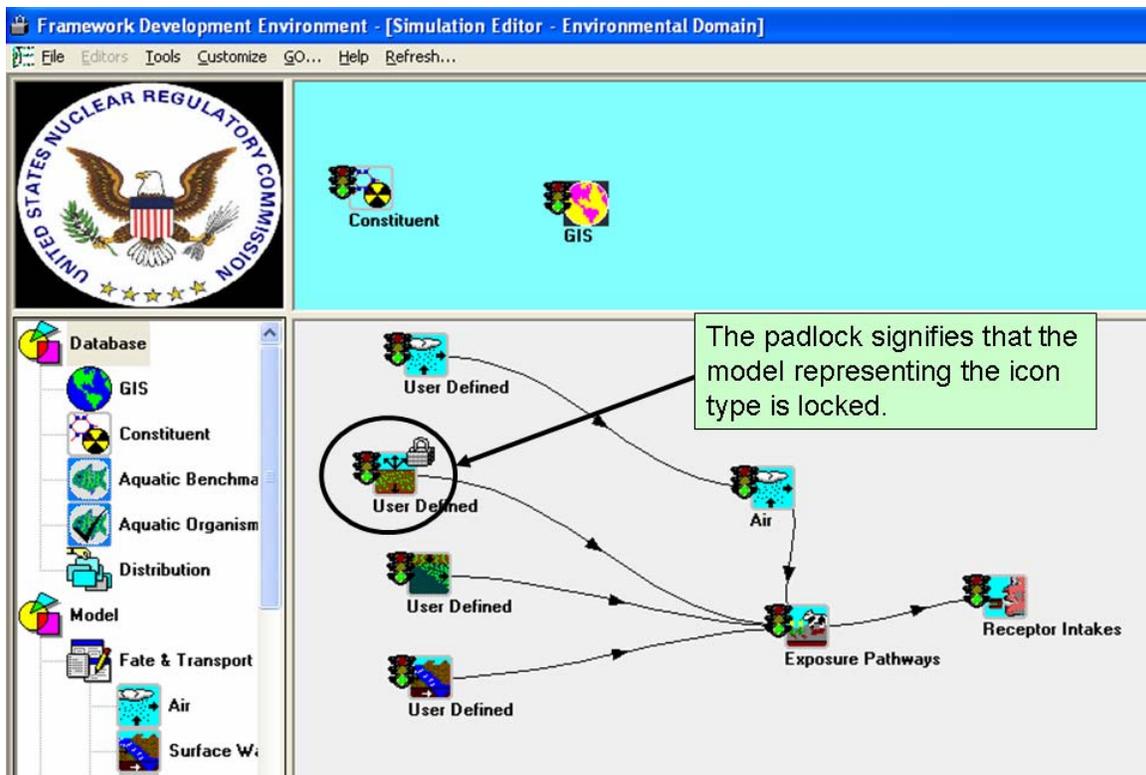
Figure 3.13. Screen Capture Illustrating the Picture of a Padlock Associated with an Icon when the Model Representing the Icon Type Is Locked
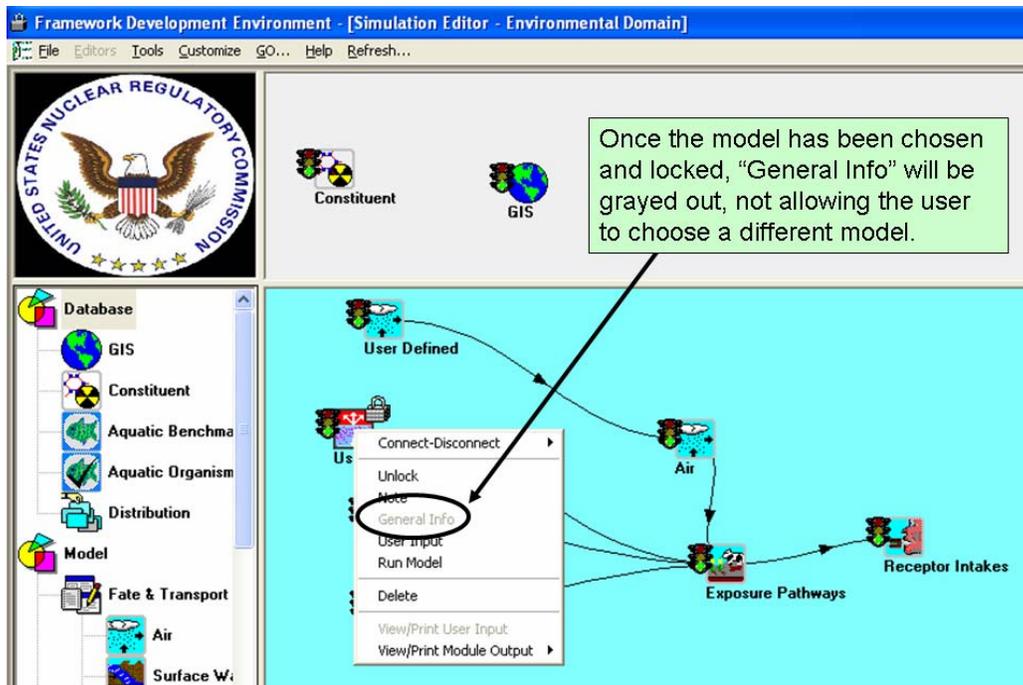
Figure 3.14. Screen Capture of the Right-Click Menu Signifying that when a Model Representing an Icon Type Is Locked, then the User Will Not Have Access to General Information

3.4 Limitations and Issues

Client-side modifications, involving the FDE, provide the user with the ability to limit the number of models associated with a Domain, lock CSMs, and assign specific models to icon types. Locking/unlocking on the server side is more involved and would require more effort, but this makes sure that virtually no one could subvert the system.

For server-side modifications, the FRAMES user interface would have to be modified for error handling and implement only a select few of the visual cues (e.g., picture of a padlock when items have been locked) outlined under the Client-side Modifications. This is because the SystemIO.dll will do most of the work, and modifications to the FRAMES FDE will be only modified to issue error messages when locked items are accessed and unable to be modified.

3.4.1 Accessing Lock and Unlock Design

As noted earlier, the user can define which models are associated with a Domain by registering those models with the Domain. As with the Client-side modifications, the Server-side modifications also provide the user with the ability to lock the models that are associated with the Domains such that a user would not be able to add or remove any of the models available to icons in the CSM Simulation. Access is granted and protected with a password. Access to locking models in the Domains would occur through the Tools menu in FRAMES, as

illustrated in Figure 3.15. The ability to access the locking protocol for the CSM Simulation and Models associated with the individual icons in the CSM are also depicted in Figure 3.15. This is accomplished by defining module files under the Tools menu, having the names "Lock Unlock Domain," "Lock Unlock Simulation," and "Lock Unlock Module." Each locking/unlocking call (which is actually represented by a "module" that is defined in the Module Editor) shall make the appropriate call to the SystemIO.dll to lock or unlock the appropriate object, Domain, Simulation, or Module. The Simulation Editor would be modified to refresh a CSM picture after a Tool menu item (i.e., "Lock Unlock Domain," "Lock Unlock Simulation," or "Lock Unlock Module") has been run. The refresh will then make the appropriate calls to enable the editor to respond with the correct visual cues.
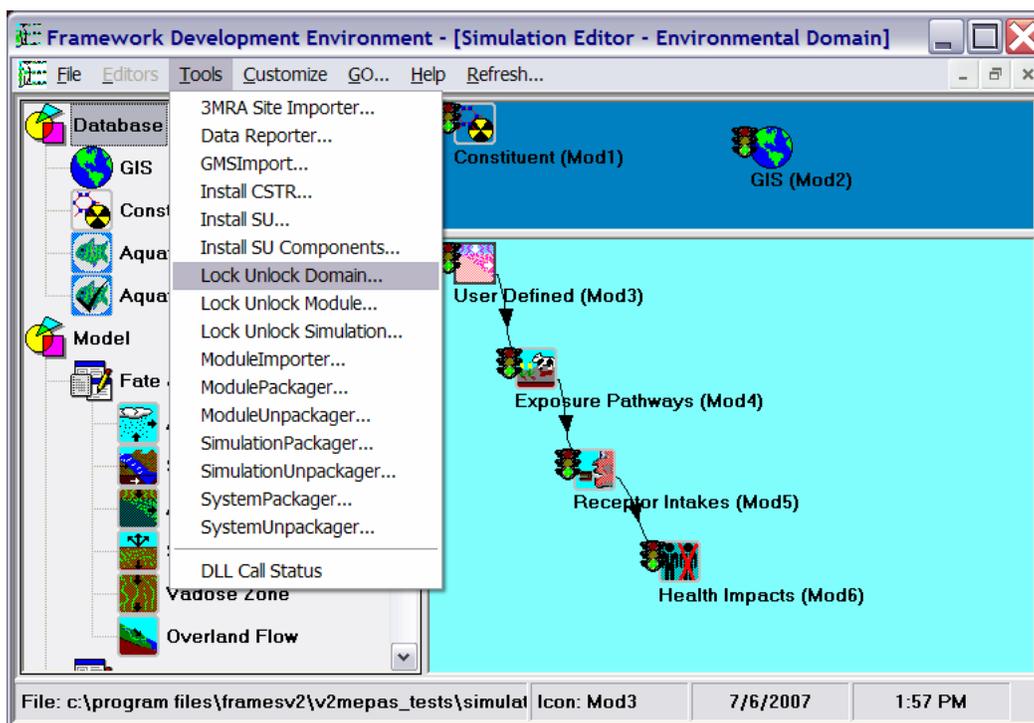
Figure 3.15. Tools Menu Containing the Locking Mechanism Options for the Server-Side Modifications

3.4.2 Dictionary, Module, and Domain Editor Design Changes

If the server-side design were to be implemented, no buttons or controls would have to be disabled in the (Units) Conversion, Dictionary, Module, and Domain Editors when the icon palette (i.e., left navigation menu) in the Simulation Editor is under a locked Domain. If the user tries to change or modify any item for a locked Domain, an appropriate error message would appear stating that the domain is locked, and no changes are possible.   This error will be generated by the SystemIO.dll itself, and the FDE will be modified to display the generated error.

3.4.3 Simulation Editor (CSM) Design Changes

Visual cues (i.e., picture of a padlock) for locking the Simulation Editor (i.e., CSM) would be the same as described under Client-side modifications.

4.0 Specifications

A specification is a defined boundary between software systems. Typical boundaries between systems include files and associated formats; in other cases, a specification may be a defined protocol that two machines will use to communicate. Often these protocols and file formats are not defined (or controlled) by the software being written but are required by the partnering software. Changes need to be made to two dictionaries: Simulation and StartUp. Tables 4.1 and 4.2 illustrate the changes to the Simulation and StartUp dictionaries, respectively. The Simulation dictionary already includes some information needed for locking, but these entries will be updated as indicated in Table 4.1. LockPassword entries will be used as a type of CRC so that a user cannot simply delete the entry to unlock the item. The Simulation LockPassword entry will change when modifying the simulation, but the StartUp LockPasssword entry will only be generated once. The Lock Connections and LockModules password entries will be an encoded string. If the CRC is missing or not correct, the simulation and all modules will be locked. The Simulation LockPassword CRC will be based on a select set of variables found in the Simulation dictionary, which are still to be determined. Password protection is always dependant on secrecy. If the method of generating the CRC key or encrypted password were published, then the protection scheme employed would be subverted.

The Password Generator uses no files.

4.1 Compiler Version

The source code that makes up the FDE.exe and PassGenerator.exe is compiled with VB 6.0.

Table 4.1. Changes to the Simulation Dictionary

Dictionary Name	Dictionary Description	Dimension	DataType	PrimaryKey	Scalar	Minimum	Maximum	Measure	Unit	Stochastic	Preposition	Index 1
LockConnections	Lock connections	0	STRING	FALSE	TRUE	0	0			FALSE		
LockModules	Lock modules	1	STRING	FALSE	TRUE	0	1			FALSE		Simulation.ModID
LockPassword	Lock password CRC	0	INTEGER	FALSE	TRUE	0	20000000			FALSE		

The StartUp dictionary will need one new entry and is indicated in Table 4.2.

Table 4.2. Changes to the StartUp Dictionary

Dictionary Name	Dictionary Description	Dimension	DataType	PrimaryKey	Scalar	Minimum	Maximum	Measure	Unit	Stochastic	Preposition	Index 1
LockPassword	Lock password CRC	0	INTEGER	FALSE	TRUE	0	20000000			FALSE		

5.0   Testing Approach and Results

The test-procedure summary includes as a minimum the date, name of tester, and the version. The target requirements should be clearly identified. Other information that is helpful and may be appropriate to add to the test procedure summary is start time, end time, and location of the test. If there are any regulations or change-request documentation related to the test, that information should also be noted in the summary of the test procedure.

5.1   Pass/Fail Test Criteria

Test criteria should be defined before testing. A standard set of nomenclature needs to be identified and documented. The standardization explanation needs to be archived with the test procedures so that future assessors can fully understand the measurement system used for the test. An explanation of what success means and what failure means is critical for the defensiveness of the test.

5.1.1   Test-Procedure Components

A log of the test should be documented containing information on the steps needed to demonstrate the requirement, expected results, and requirement-specific criteria to be used to determine a pass or fail finding. Related comments and documentation should also be captured. It is very valuable to identify the documents used to support the understanding and expectation of the requirement (e.g., statement of work, user's guide, help file). This identification of related documentation helps to tie together the quality documentation package for future readers of the procedure.

When designing the flow of a testing procedure, there are several types of requirements that can be grouped to facilitate testing. Some standard categories are functional requirements, data flow, calculations, output checks, and user-scenario cases.

1. Functional Requirements—Based on the client requirements describing what functions exist in each component of the system.

2. Data Flow—Flow of information between users, database tables, modules, displays, and the output produced.

3. Calculations—Any processing of module/display values. This includes unit conversions. Any data transformation should be documented and tested for the system.

4. Output Check—Confirmation of the correct generation of the output products.

5. Additional Scenarios—Scenarios that are developed to provide some holistic assessment of cases that may be possible and relevant to the expected use of the product.

Other information, such as prerequisite requirements, inputs, and assumptions, can also be collected and should be documented if they exist. Other supporting tools should be considered where appropriate. Tools such as change-tracking systems and automated testing tools are helpful in sustaining a quality testing process.

All tests assume that the Frames V2 and the Groundwater Modeling System (GMS) 5.0 has been installed and that the tutorial case file exists. The latest FramesV2 installation can be found on CoLab at
https://colab.sc.egov.usda.gov/cb/displayDocument/FramesV2Setup.exe?doc_id=2744.

5.2 Example #1: Locking/Unlocking Domain, CSM, Model, Using RT3DTutObs.sim

Description: Three different locking mechanisms have been developed with the purpose of restricting user access to making modifications, changes, additions, and deletions associated with models and CSMs in FRAMES. Three locking options are summarized as follows: 1) models associated with a Domain, 2) CSM simulation, and 3) model associated with an icon type. All requirements associated with each locking mechanism are tested, and only one test case is required to demonstrate that each locking/unlocking mechanism works as designed. The RT3D Test Case #2, as described in detail by Whelan et al. (2007) and as presented in Figure 5.1, is used to test the three locking/unlocking mechanisms.
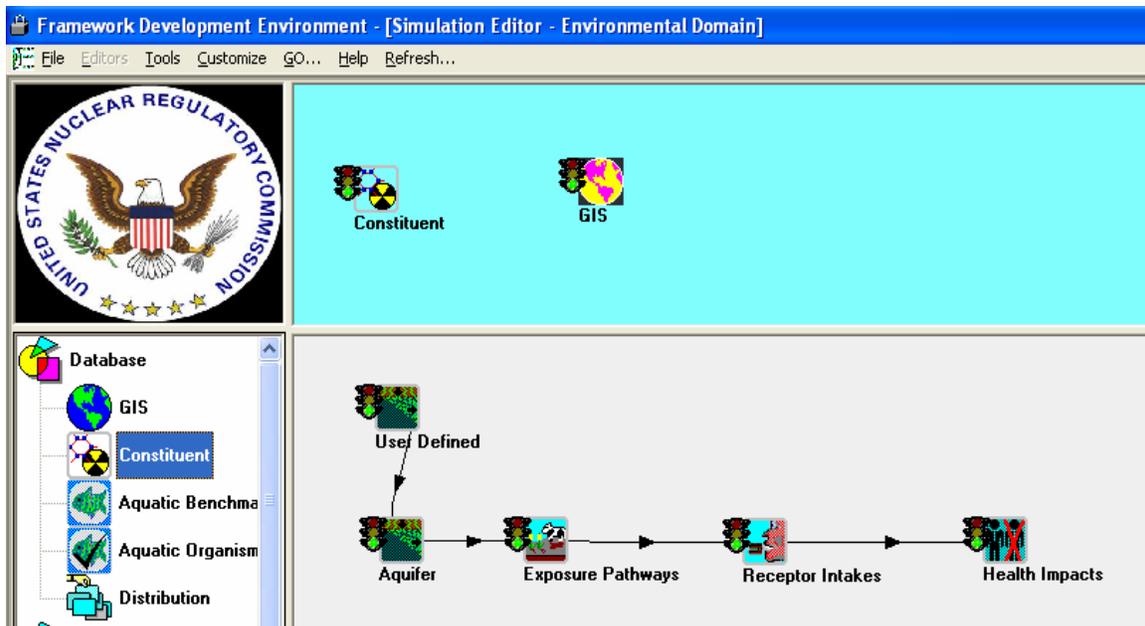

Figure 5.1. RT3D Test Simulation RT3DTutObs

5.2.1 Input Data

The input data refer to the locking/unlocking mechanism and do not specifically refer to data entered by the user in the GMS Import tool and in the Data Client Editor (DCE) for the RT3D aquifer module or other models associated with the CSM, as described by Whelan et al. (2007). It is assumed that the reader will refer to Whelan et al. (2007) for each model's input when the test case is run to completion. Only those entries associated with the locking mechanism are provided in the section titled "Conducting the Test."

Expected Results: The expected results are that

1. models associated with the Domain will be locked when designated. When unlocked, the user will have the ability to add, remove, or modify models or their attributes using the editors (i.e., [Units] Conversion, Module, Domain, and Dictionary).

2. the CSM will be locked when designated. When unlocked, the user will have the ability to add, remove, or modify icons and the connections associated with icons.

3. the specific model of an icon will be locked when designated. When unlocked, the user will have the ability to choose a different model to represent the icon.

5.2.2 Conducting the Test

Because the RT3DTutObs test case is imported through the GMS Import tool, which uses the SystemIO.DLL, RT3DTutObs is imported regardless of the locks on the Domain. This is an example of where the server-side modifications would prevent this import, if locked. The locking mechanism only works if one modifies the system through the FDE user interface.

Importing the RT3DTutObs Test Case

1. Install the GMS models of interest. For RT3D, this includes RT3D.exe (Version 2.5) and RXNS.dll. For the Modular Three-Dimensional (MT3D) model, this includes MT3DMS4.exe (Version 4.0). These files should be added to the following directory, which is the default: C:\Program Files\GMS50\models. If GMS 5.0 is already installed, then this step is not required.

2. Extract the latest version of the GMS Import tool if available. The latest version can be found on COLAB:
https://colab.sc.egov.usda.gov/cb/displayDocument/GMSUpdate.zip?doc_id=35261.
Extract all contents to the C:\Program Files\FramesV2\GMS directory, provided C:\Program files\FramesV2 was the FRAMES installation directory.

3. Start the FRAMES 2.0 Framework Development Environment (if it is not already up).

4. If the "Simulation Editor" is started, you will need to close that by choosing File → Exit from the menu.

5. Follow the remaining instructions outlined by Whelan et al. (2007) for registering and importing the RT3DTutObs test case.

Testing the Mechanism to Lock/Unlock Models Associated with the Domains

1. If not in the FDE user interface, return to the FDE user interface. Note that the current state of the Domains is locked, as denoted by the padlock in the upper left-hand corner.

2. Unlock the Domain by left-clicking the File menu and choosing Unlock System, as illustrated in Figure 3.3a. A password text box, similar to that shown in Figure 3.4, appears.

3. Type in the machine- and time-dependent password, which was generated by the Password Generator. The Password Generator is an independent software product specifically designed to generate passwords for unlocking the Domain.

4. If the Password Generator is in possession, run the executable. A screen will appear, similar to the bottom right-hand figure in Figure 3.6. Go to Help → About on the menu bar, and obtain the Installation CRC number, which is required to generate the password. Input the correct Installation CRC number, and return a password. Run the Password Generator again, but enter a fictitious number. An error message is returned, like the one in Figure 3.7.

5. When the password is successfully accepted, the padlock in the upper left-hand corner is replaced by the FRAMES-2 symbol, and under the File menu, "Unlock System" is replaced by "Lock System," as illustrated in Figure 3.3b.

6. Under Editors on the menu bar, choose Environmental Domain. In the upper left-hand corner, a picture of a padlock appears, as illustrated in Figure 3.2. This signifies that the Domains are locked, and new models cannot be added or removed.

7. Exit the CSM by choosing Exit under File on the menu bar, and return to the FDE interface.

8. Under File on the menu bar, choose "Lock System," as illustrated in Figure 3.3b. The padlock automatically appears in the upper left-hand corner, signifying that the Domain is locked. No password is required as this is a system-generated (not user-generated) password.

9. Under the Editors menu, open the Module Editor, as illustrated in Figure 3.5. The user has the flexibility to navigate throughout the editors, but all of the active buttons have been grayed out. Exit the Module Editor by choosing Close.

Testing the Mechanism to Lock/Unlock the CSM

1. Under the Editors menu, choose Environmental Domain.

2. Under the File, Open menu, open RT3DObsTut.sim. Note that the upper-most, left-hand symbol is that of a padlock, signifying that the Domains are locked. The symbol below it (in the upper left-hand corner) is that of the FRAMES-2 symbol, signifying that the CSM is unlocked. See Figure 5.1.

3. Under File in the menu bar, as illustrated in Figure 3.9, choose Lock from the menu.

4. A box will appear requiring the user to define a password, as illustrated in Figure 3.10.

5. After successfully entering a password, two padlocks will appear in the upper left-hand corner, as illustrated in Figure 5.2. The top-most padlock indicates that the Domain is locked, and the one just below it indicates that the CSM is locked.

6. Attempts to add, delete, and disconnect icons were unsuccessful. An error message is displayed, as illustrated in Figure 5.3. The icons can be repositioned on the screen.

7. Under the File menu bar, choose Unlock from the menu. The user will be prompted to supply a simulation password. When successful, icons can be added, deleted, and disconnected. Note that one of the padlocks (i.e., second one down) in the upper left-hand corner returns to a picture of the FRAMES-2 symbol, as illustrated in Figure 5.1.
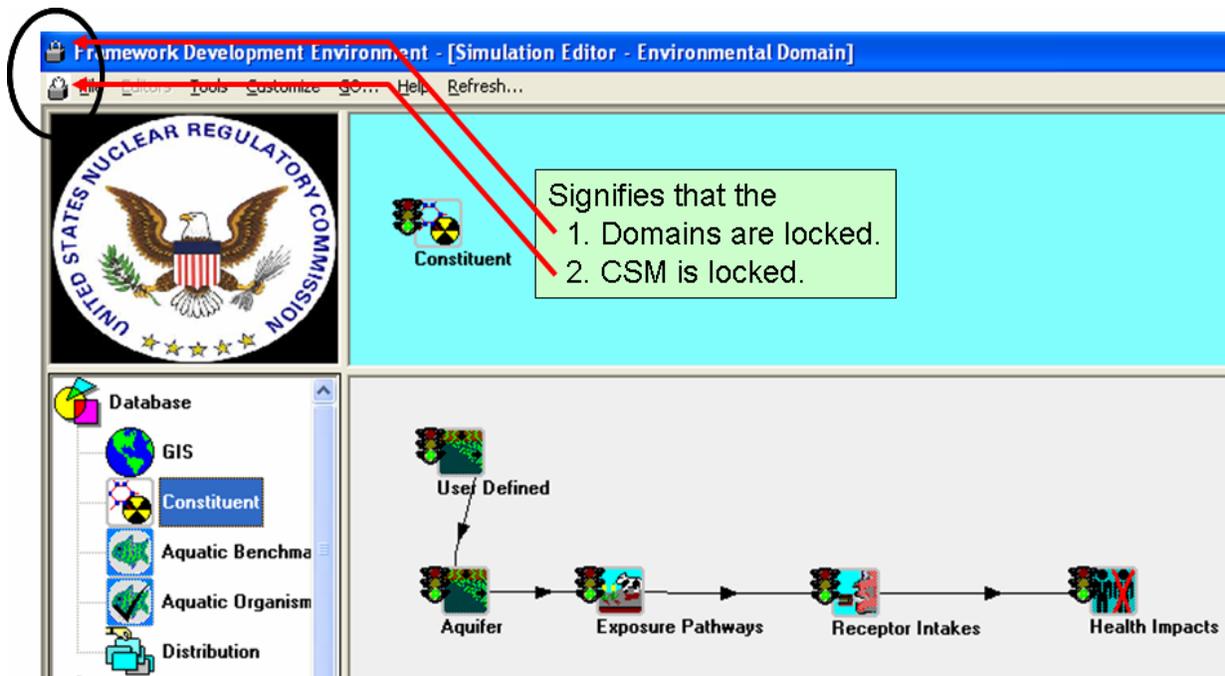

Figure 5.2. Screen Capture Illustrating that the Domains and CSM Are Locked, as Signified by the Padlocks

Figure 5.3. Error Message when the CSM Is Locked and the User Attempts to Modify the Picture

Testing the Mechanism to Lock/Unlock a Model Associated with the Aquifer Icon

1. Right-click the aquifer icon, and choose General Info from the menu, similar to the menu that appears in Figure 3.11.

2. Of the model choices, choose RT3DTutObs, as illustrated in Figure 5.4. Save and Exit.

3. Right-click the aquifer icon, and choose Lock from the menu, similar to the menu that appears in Figure 3.11.

4. A box will appear requiring the user to define a password, as illustrated in Figure 3.12a.

5. After successfully entering a password, a padlock will appear in the upper right-hand corner of the Aquifer icon, as illustrated in Figure 5.5.

6. Right-click the aquifer icon. Note that General Info from the menu is grayed out, so the user cannot choose a different model to represent the icon, as illustrated in Figure 5.6

7. Choose Unlock, as shown in Figure 5.6. A screen similar to Figure 3.12b appears. Enter the same password used in Steps 4 and 5. The padlock disappears, and a screen similar to Figure 5.1 reappears.
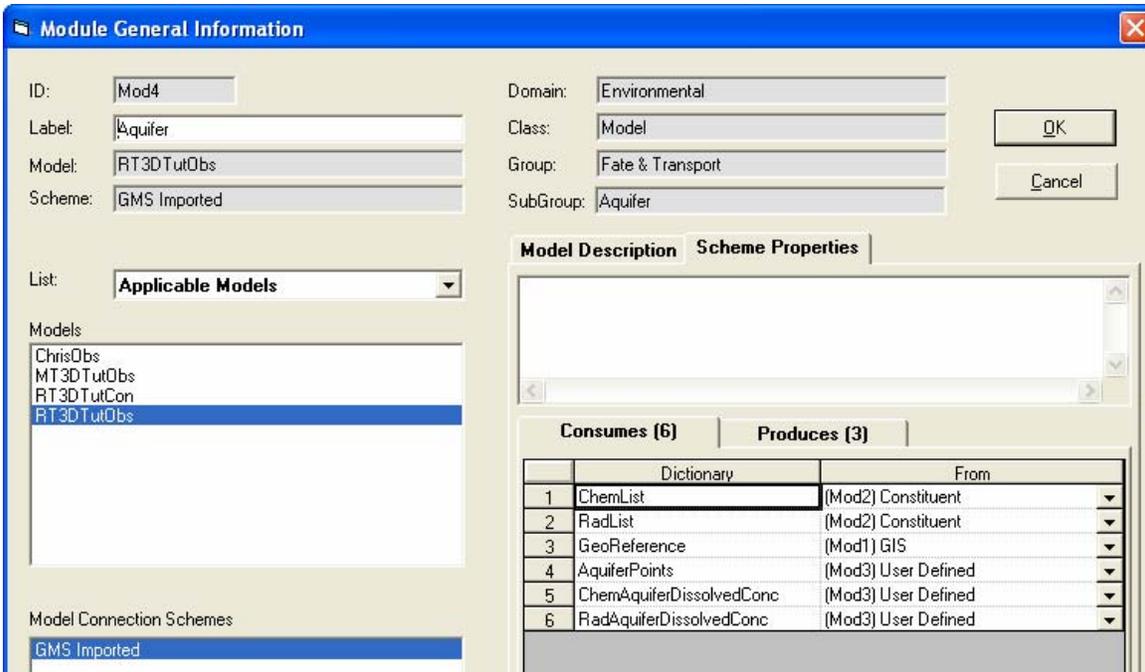
Figure 5.4. General Info Screen for the Aquifer Icon in the RT3DTutObs.sim CSM
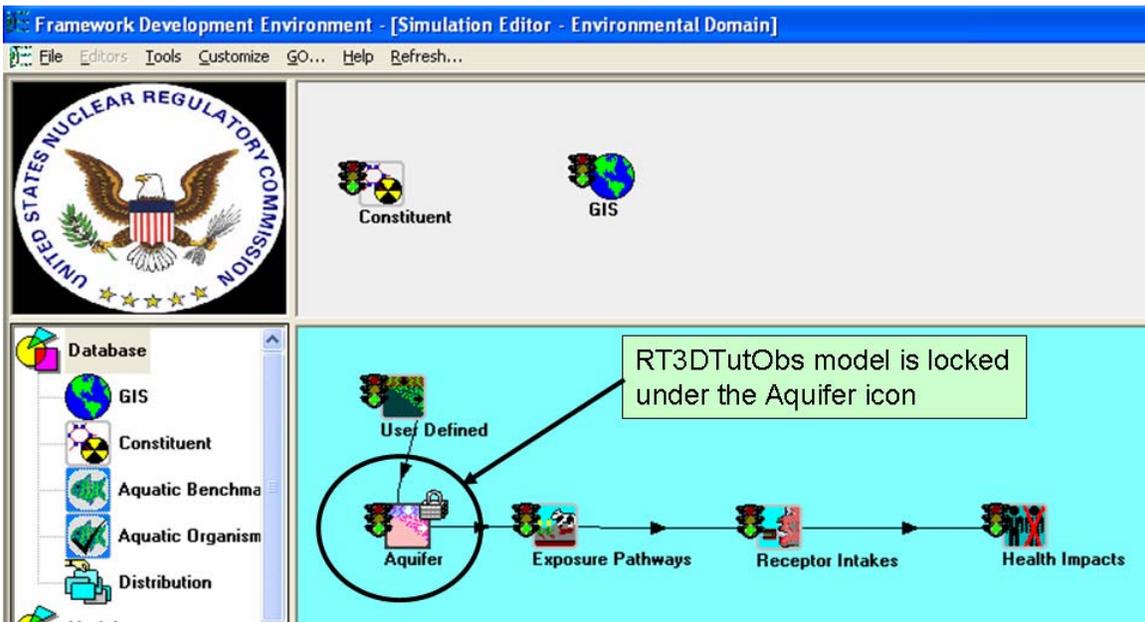

Figure 5.5. Screen Capture Illustrating a Locked Model with the Aquifer Icon, Designed by a Padlock on the Aquifer Icon
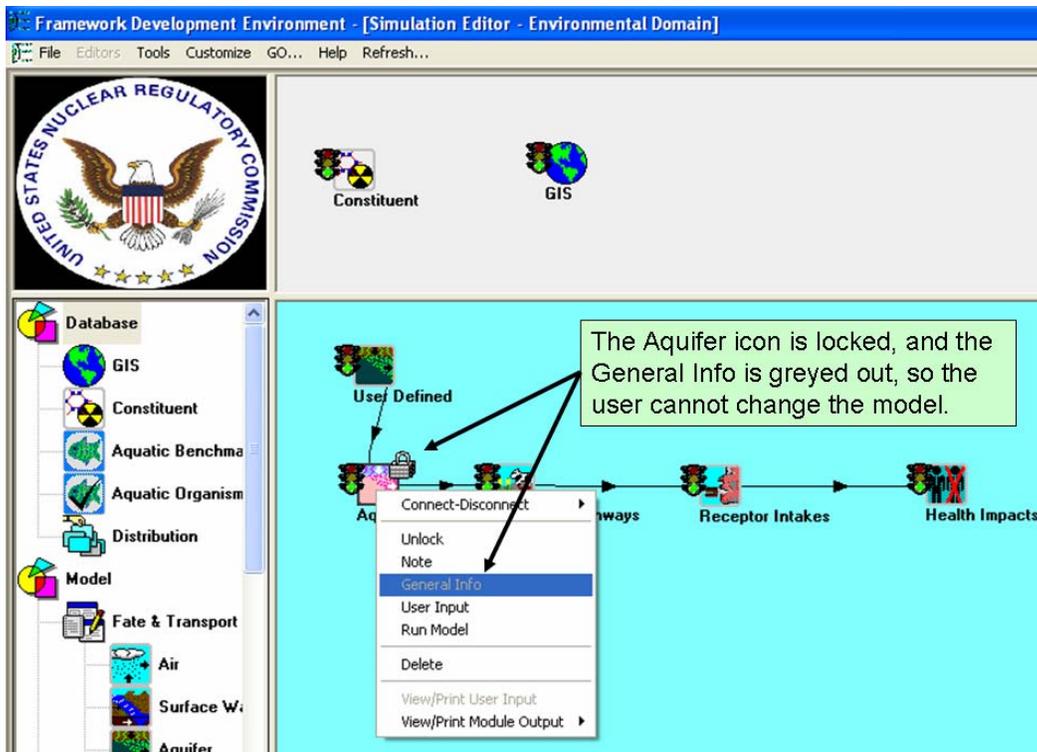
Figure 5.6. Screen Capture Illustrating that the Model Cannot Be Changed when the Icon is Locked

5.2.3 Results

All requirements are met, and all locking and unlocking functionalities work as designed.

6.0 Bibliography

Army Corps of Engineers (ACOE). 2007. *Adaptive Risk Assessment Modeling System (ARAMS)*. Engineer Research and Development Center, Vicksburg, Mississippi. Available at: http://el.erdc.usace.army.mil/arams/. Accessed August 3, 2007.

U.S. Environmental Protection Agency (EPA). 2007a. *Hazardous Waste Identification Rule Assessment*. National Exposure Research Laboratory, Research Triangle Park, North Carolina. Available at: http://www.epa.gov/nerl/factsheets/2001/goal5_assessment.pdf. Accessed August 3, 2007.

U.S. Environmental Protection Agency (EPA). 2007b. *Supercomputer for Model Uncertainty and Sensitivity Evaluation.* Ecosystems Research Division, Athens, Georgia. Available at: http://www.epa.gov/athens/research/modeling/supermuse/supermuse.html. Accessed August 3, 2007).

Whelan, G., K.J. Castleton, and M.A. Pelton. 2007. *FRAMES-2.0 Software System: Linking to the Groundwater Modeling System (GMS) RT3D and MT3DMS Models*. PNNL-16758, Pacific Northwest National Laboratory, Richland, Washington.

Whelan G., K.J. Castleton, M.A. Pelton, and R.Y. Taira. 2006. *Concepts Associated with Transferring Temporal and Spatial Boundary Conditions between Modules in the Framework for Risk Analysis in Multimedia Environmental Systems (FRAMES)*. PNNL-16145. Pacific Northwest National Laboratory, Richland, Washington.

Whelan G, KJ Castleton, JW Buck, GM Gelston, BL Hoopes, MA Pelton, DL Strenge, and RN Kickert. 1997. *Concepts of a Framework for Risk Analysis in Multimedia Environmental Systems (FRAMES)*. PNNL-11748, Pacific Northwest National Laboratory, Richland, Washington.

6.1 Documentation for the FRAMES-3MRA Technology Software System

Volume 1: *Overview of the FRAMES-HWIR Technology Software System.* 1998. PNNL-11914, Vol. 1, Pacific Northwest National Laboratory, Richland, Washington.

Volume 2: *System User Interface Documentation.* 1998. PNNL-11914, Vol. 2, Pacific Northwest National Laboratory, Richland, Washington.

Volume 3: *Distribution Statistics Processor Documentation.* 1998. TetraTech, Lafayette, California.

Volume 4: *Site Definition Processor Documentation.* 1998. PNNL-11914, Vol. 4, Pacific Northwest National Laboratory, Richland, Washington.

Volume 5: *Computational Optimization Processor Documentation.* 1998. TetraTech, Lafayette, California.

Volume 6: *Multimedia Multipathway Simulation Processor Documentation.* 1998. PNNL-11914, Vol. 6, Pacific Northwest National Laboratory, Richland, Washington.

Volume 7: *Exit Level Processor Documentation.* 1998. PNNL-11914, Vol. 7, Pacific Northwest National Laboratory, Richland, Washington.

Volume 8: *Specifications.* 1998. PNNL-11914, Vol. 8, Pacific Northwest National Laboratory, Richland, Washington.

Volume 9: *Software Development and Testing Strategies.* 1998. PNNL-11914, Vol. 9, Pacific Northwest National Laboratory, Richland, Washington.

Volume 10: *Facilitating Dynamic Link Libraries.* 1998. PNNL-11914, Vol. 10, Pacific Northwest National Laboratory, Richland, Washington.

Volume 11: *User's Guidance.* 1998. PNNL-11914, Vol. 11, Pacific Northwest National Laboratory, Richland, Washington.

Volume 12: *Dictionary.* 1998. PNNL-11914, Vol. 12, Pacific Northwest National Laboratory, Richland, Washington.

Volume 13: *Chemical Properties Processor Documentation.* 1998. PNNL-11914, Vol. 13, Pacific Northwest National Laboratory, Richland, Washington.

Volume 14: *Site Layout Processor Documentation.* 1998. PNNL-11914, Vol. 14, Pacific Northwest National Laboratory, Richland, Washington.

Volume 15: *Risk Visualization Tool Documentation.* 1998. PNNL-11914, Vol. 15, Pacific Northwest National Laboratory, Richland, Washington.

6.2 Quality Assurance Program Document

Gelston GM, RE Lundgren, JP McDonald, and BL Hoopes. 1998. *An Approach to Ensuring Quality in Environmental Software*. PNNL-11880, Pacific Northwest National Laboratory, Richland, Washington.

6.3 Additional Sources

Buck JW, BL Hoopes, KJ Castleton, and RY Taira. 1999. *Requirements for the FRAMES User Interface*. PNNL-SA-32277, Pacific Northwest National Laboratory, Richland, Washington.

Draper N, and H Smith. 1981. *Applied Regression Analysis*. 2nd ed, John Wiley and Sons, New York.

U.S. Environmental Protection Agency (EPA). 1997. *System Design and Development Guidance*. EPA Directive Number 2182, Washington, D.C.

Faraway JJ. *Practical Regression and Anova Using R*. Available at: http://cran.r-project.org/doc/contrib/Faraway-PRA.pdf. Accessed August 3, 2007.

Gelston, GM, RE Lundgren, KJ Castleton, RY Taira, TE Swanson, JP Mcdonald, and BL Hoopes. 2006. *Software Integration Frameworks: An Approach to Ensuring Quality*. PNWD-3776. Pacific Northwest National Laboratory, Richland, Washington.

Gelston GM, RE Lundgren, JP McDonald, and BL Hoopes. 1998. *An Approach to Ensuring Quality in Environmental Software*. PNNL-11880, Pacific Northwest National Laboratory, Richland, Washington.

Gelston GM, MA Pelton, R Lundgren, KJ Castleton, G Whelan, BL Hoopes, J . Kirk AJ Pospical, M Eslinger, JG Droppo, Jr., and DL Strenge. 2004. *Documentation for the Dictionary Editor of the FRAMEwork System (FRAMES)*. PNWD-3504, Pacific Northwest National Laboratory, Richland, Washington.

Hoopes BL, MA Pelton, KJ Castleton, GM Gelston, G Whelan, RY Taira. 2004. *Documentation for the FRAMEwork Development Environment*. PNWD-3509, Pacific Northwest Laboratory, Richland, Washington.

Neter J, W Wasserman, and MH Kutner. 1985. *Applied Linear Statistical Models*. 2nd ed., Homewood, Ill., Richard D. Irwin, Inc. pp. 288-290, 417-444, 508.

Office of Civilian Radioactive Waste Management (OCRWM). 1995. *Quality Assurance Requirements and Description, Supplement I, Software*. U.S. Department of Energy, Washington, D.C.

U.S. Environmental Protection Agency (EPA). 1997. *System Design and Development Guidance*. EPA Directive Number 2182, Washington, D.C.