

# CAIRIS User Manual

Shamal Faily

July 11, 2010

Revision: \$URL: svn://edison.comlab.ox.ac.uk/res08/iris/doc/manual.txt \$ \$Id: manual.txt  
294 2010-07-11 18:38:35Z shaf \$

## Part I

# Getting started with CAIRIS

## 1 The problem

You don't have to go far to hear about security problems in software. Tales of lost data, viruses, and cyberwarfare are now fairly common in the media. Similarly, we all have experiences of using software which are less than pleasurable, especially where security is concerned; we have to remember lots of different passwords and, in some cases, are bombarded with security controls which can get in the way of the tasks we need to carry out.

Many of the reported problems arise because security is designed as an after-thought; security controls were added to an existing architecture derived from a requirements analysis which didn't take into account security concerns. In principle, all we need to do to start building secure systems is analyse security concerns in concert with requirements engineering activities. In practice, this begs the question of how we actually analyse security concerns in concert with requirements engineering. The more we look at this question, the more we find more questions than answers. How do we reconcile functional goals with quality goals such as security and usability? If we have some pre-conceived ideas about possible threats and vulnerabilities, how do we use this information to augment our analysis? How do we manage and reason about all this information and build a specification that can be used as a basis of a secure architecture?

If we devise a means of answering these questions, will the resulting requirements specify a system which is not just secure, but usable as well? The answer might well be 'it depends': it depends on the contexts within which the system will be used, how reflective the needs of the contributing stakeholders are to the people that will actually use the system, and how much the security controls help or hinder the activities that people will use the system for. Existing approaches for Security Requirements Engineering don't really think about these questions; they assume we will specify a system for a single environment and, by virtue of stakeholder contribution to the requirements process, these system will be usable for the 'user'. In reality, the environments within which a system is situated are liable to change, as are the goals and motivations of the people using it. The process of eliciting requirements for secure system also need to encompass techniques to ensure the system is 'user-centered'.

## 2 What is CAIRIS?

CAIRIS stands for Computer Aided Integration of Requirements and Information Security. At a superficial level, CAIRIS is a requirements management tool. However, unlike traditional Requirements Management tools, CAIRIS is not agnostic about the sort of systems it is used to specify: we assume that you want to use CAIRIS to specify a system needing to be secure and usable. Because of this CAIRIS, doesn't support the sort of ad-hoc extensibility that you will find in more generic tools like DOORS or Requisite Pro: it doesn't need to. The important traceability links between artifacts specified in CAIRIS are automatically maintained, and, because of this, on-going work can be automatically analysed and visualised.

CAIRIS is part of the IRIS (Integrating Requirements and Information Security) Framework. This framework was devised to provide a means of eliciting requirements for secure and usable systems. The easiest way to conceptualise IRIS is in different layers, as illustrated in Figure fig:FrameworkLayers (Figure 1). At the bottom layer is the IRIS meta-model; this is a conceptual model which describes how components from Requirements Engineering, Usability Engineering, and Information Security relate to each other. The top layer is the

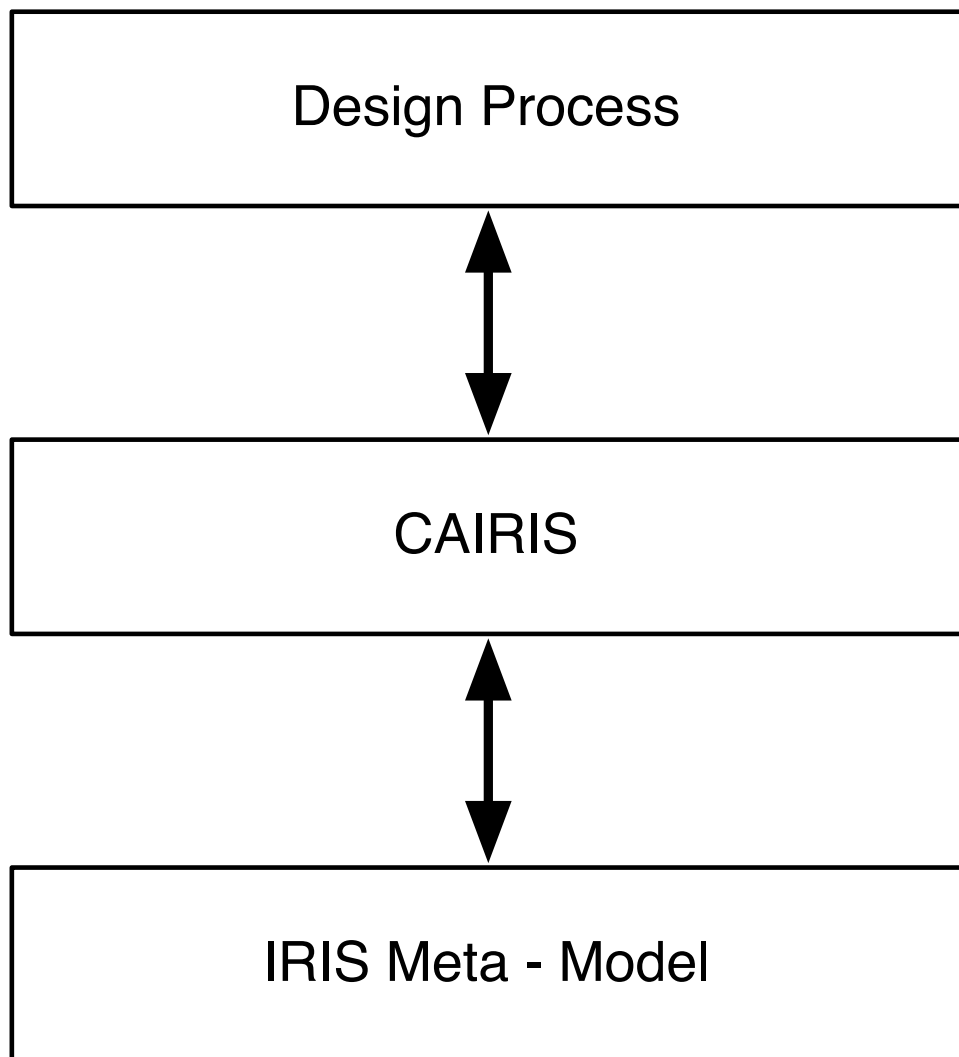


Figure 1: IRIS Framework

design process for eliciting, analysing, and specifying requirements. Between these 2 layers lies CAIRIS.

CAIRIS was designed to be used in conjunction with a design process eliciting the elements of the IRIS meta-model; if these elements are captured and entered into CAIRIS, the tool will analyse the impact this data has to security and usability of the emergent specification. At any point, the analysis stored in CAIRIS can be serialised as a requirements specification. A high-level activity diagram of this provided in figure fig:IRISActivity (Figure 2).

The specifics of the design process aren't important for this document. Indeed, if you so wish, you can simply use CAIRIS to manage requirements, model assets or goals, or perform simple risk management. However, as you read this document, you will discover that all of these activities are self-reinforcing. Specifying tasks can help you get better handle on system goals and requirements, which we can 'break' to help discover threats, vulnerabilities, and eventually risks, in our specifications. If you find yourself using the different parts of CAIRIS in a complementary manner, it is likely that you are implicitly following the IRIS design process.

### 3 Pre-requisites

Before CAIRIS can be used, recent version of the following open-source applications need to be installed:

- Python
- MySQL Community Server and Client
- MySQLdb
- GraphViz
- pyparsing
- PyDot
- NumPy
- wxPython
- Glade
- DocBook
- dblatex

In theory, CAIRIS will run on any platform which supports Python and above pre-requisites. In practice, however, running all of these pre-requisites on any operating system other than Linux might be a bit of a challenge. Therefore, we recommend that CAIRIS is used only on Linux. We have tested CAIRIS using recent versions of Red Hat and Ubuntu. In particular, all of the pre-requisites are available via Ubuntu's Synaptic Package Manager.

### 4 Obtaining CAIRIS

A source distribution of CAIRIS can be downloaded by clicking on the Download link at <http://www.comlab.ox.ac.uk/cairis>.

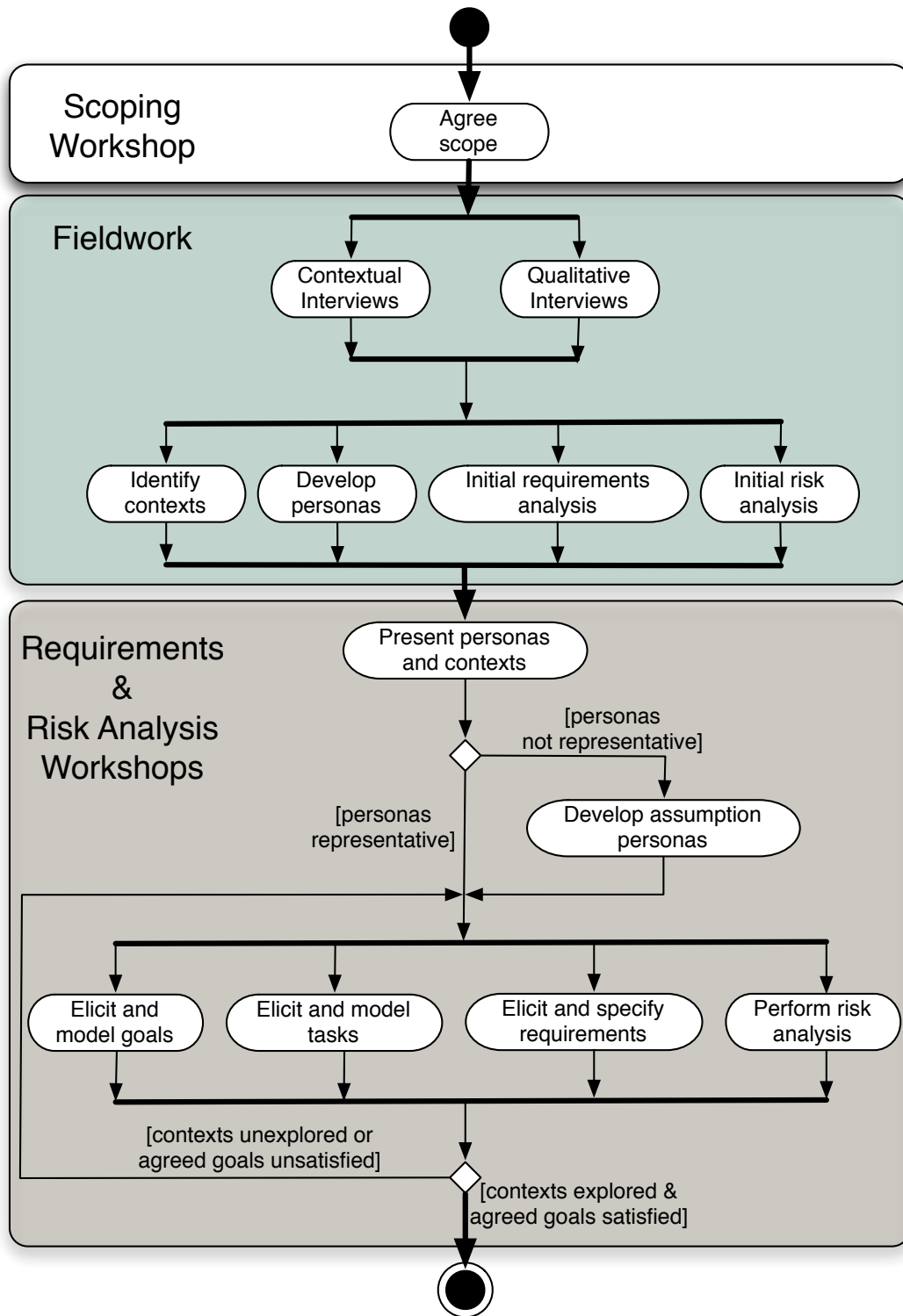


Figure 2: Activity diagram of IRIS design process

Table 1: IRIS directory tree

Directory	Description
examples	Sample project files
doc	CAIRIS documentation (including this manual)
iris/iris	CAIRIS source code, including start-up script
iris/sql	SQL scripts used by CAIRIS
iris/images	Image files used by CAIRIS
iris/config	CAIRIS run-time configuration data

Following checkout, the following directories are created beneath the root iris directory:

## 5 Installing CAIRIS

### 5.1 Environment variables

A number of environment variables are used by CAIRIS at run-time; these are defined in table IRIS Environment variables (Table 2). These must to be set before CAIRIS can be started.

Table 2: IRIS Environment variables

Directory	Description
IRIS_BACKUP	Default directory for storing CAIRIS project files
IRIS_SCRATCH	Temporary files directory
IRIS_CONFIG	Location of IRIS configuration data
IRIS_IMAGES	Location of icon files used by CAIRIS
IRIS_SRC	Location of IRIS source files

We recommend setting IRIS\_CONFIG, IRIS\_IMAGES, and IRIS\_SRC with the current locations of iris/config, iris/images, and iris/iris respectively. We also suggest using /tmp for the location of IRIS\_SCRATCH.

### 5.2 Database setup

CAIRIS stores its data in a MySQL database. An empty database needs to be created, and an account associated with it, before the CAIRIS can be started. When this database is created, a file called *db.ini* must be created. This file shall contain the following 5 lines:

line 1. The database server network location, e.g. 127.0.0.1  
line 2. The database server port, e.g. 3306  
line 3. The database user, e.g. irisuser  
line 4. The database password  
line 5. The database name, e.g. iris

This file needs to be saved in the iris/iris directory. A sample db.ini file is included in the iris/iris directory of the CAIRIS source distribution.

Using mysql, it is also necessary to run 2 SQL scripts in the iris/sql directory. The init.sql script creates the CAIRIS database table, and populates the database with meta-

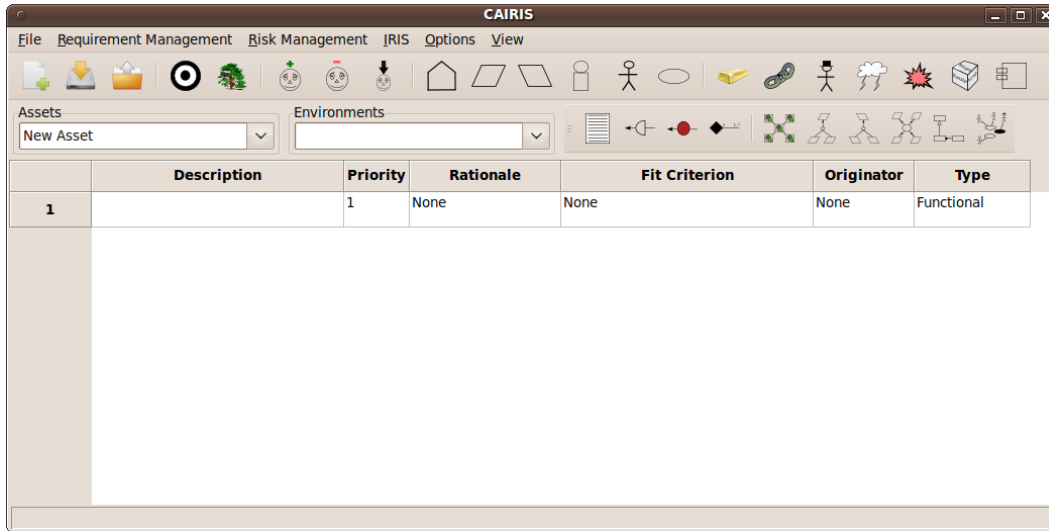


Figure 3: An empty CAIRIS project

data needed by the tool. The `procs.sql` script creates a number of stored procedures and database functions used by CAIRIS. These scripts can be run from the mysql prompt, i.e.

```
> mysql -h localhost -u irisuser -password="irispaword" iris < iris/sql/init.sql
> mysql -h localhost -u irisuser -password="irispaword" iris < iris/sql/procs.sql
```

Finally, because a number of the CAIRIS stored procedures are recursive, it is necessary to modify the database server to support recursion. This support can be added by running the following command:

```
> mysql -h localhost -u root << !
set global max_sp_recursion_depth = 255;
flush tables;
flush privileges;
!
```

Where *localhost* corresponds to the location of the database server.

## 6 Starting CAIRIS

To start CAIRIS, run the `$iris.py$` script in the `iris/iris` directory. If this is the first time CAIRIS has been run and the CAIRIS database is empty, CAIRIS should look like `fig:initStartup` (Figure 3).

This main CAIRIS window is split in 2 halves. The bottom half is taken up by the requirements editor, which is described in more detail in section `adding, updating, and deleting requirements` (section 15.5).

The top half of the screen is taken up by the menu and tool-bar buttons. A key for the toolbar buttons is provided in figure `fig:toolKey` (Figure 4).



Icon	Action	Menu Path
	New Project	File / New
	Save Project	File / Save
	Open Project	File / Open
	Edit Project Settings	---
	Edit Environments	IRIS / Environments
	Add Requirement	Requirement Management / Add
	Delete Requirement	Requirement Management / Delete
	Commit latest Requirement changes	Requirement Management / Commit
	Edit Domain Properties	IRIS / Domain Properties
	Edit Goals	IRIS / Goals
	Edit Obstacles	IRIS / Obstacles
	Edit Roles	IRIS / Roles
	Edit Personas	IRIS / Personas
	Edit Tasks	IRIS / Tasks
	Edit Assets	Risk Management / Assets
	Edit Vulnerabilities	Risk Management / Vulnerabilities
	Edit Attackers	Risk Management / Attackers
	Edit Threats	Risk Management / Threats
	Edit Risks	Risk Management / Risks
	Edit Responses	Risk Management / Responses
	Edit Countermeasures	Risk Management / Countermeasures
	Generate Documentation	---
	Edit Goal Associations	IRIS / Goal Associations
	Edit Asset Associations	IRIS / Asset Associations
	View Risk Analysis Model	View / Risk Analysis Model
	View Goal Model	View / Goal Model
	View Obstacle Model	View / Obstacle Model
	View Responsibility Model	View / Responsibility Model
	View Asset Model	View / Asset Model
	View Task Model	View / Task Model
	View Assumption Personas Model	View/Assumption Persona Model

## 7 Saving and opening CAIRIS project files

All the information entered into CAIRIS is stored in a single MySQL database. To save the contents of this data, click on the Save Project toolbar button and, from the save project data dialog box, enter the name of the project file and the location to store the data. The data is stored as an ASCII text SQL dump file. To open a pre-existing project file, click on the Open project toolbar button and select the profile file to open.

## 8 Sample projects

The CAIRIS source distribution comes with 3 sample project files; these are described in the table below.

Table 3: Sample project files

File name	Description
preMit.sql	An initial analysis of a software repository.
postMit.sql	A developed version of the above example.
completeExample.sql	An requirements and risk analysis of an e-Science grid

**Part II**

**Using CAIRIS**

In this part of the document, we describe step-by-step instructions on using CAIRIS' functionality.

## 9 Starting the project

The first stage of the design process involves establishing the scope of subsequent analysis. CAIRIS supports this exercise by using the Project Settings notebook.

### 9.1 Update project settings

- Click on the Project Settings button to open the Project Settings notebook. By default, the notebook will open in the Background page. Enter the project name and background in this page.
- Click on the Goals tab and enter the high-level goals of that the system being specified needs to satisfy.
- Click on the Scope tab and enter the scope of the system being specified.
- If a rich picture or context diagram has been agreed, click on the Rich Picture tab and, by right clicking on the page to bring up the Load Image option from the speed menu, select a rich picture to import. Please note that the image itself is NOT imported into the database, only the file path to the picture.
- Names or terms that the readership of the specification may be unfamiliar with can be added to the project on an on-going basis. To add a term, click on the Naming Conventions tab, right click on the name page, and select Add from the speed menu. This opens a window which allows a name and a definition to be added to the naming convention list. To modify an existing entry, double click on the entry and make the required modifications. Entries can also be deleted from the right-click speed menu.
- Clicking on the Contributors tab opens the Contributors page. To add a contributor, right click on the page and select Add from the speed menu to open the Add Contributor dialog box. Contributors can be either a participant, facilitator, or scribe; these reflect the roles that people take in participatory workshops.

## 10 Environments

An environment might represent a system operating at a particular time of day, or in a particular physical location. Environments encapsulate visible phenomena such as assets, tasks, personas, and attackers, as well as invisible phenomena, such as goals, vulnerabilities, and threats. Environments may be identified at any time, although these may not become apparent until carrying out contextual inquiry and observing how potential users reason about their context of use.

### 10.1 Adding a new environment

- Click on the Environment toolbar button to open the Environments dialog box, and click on the Add button to open the Environment dialog box.

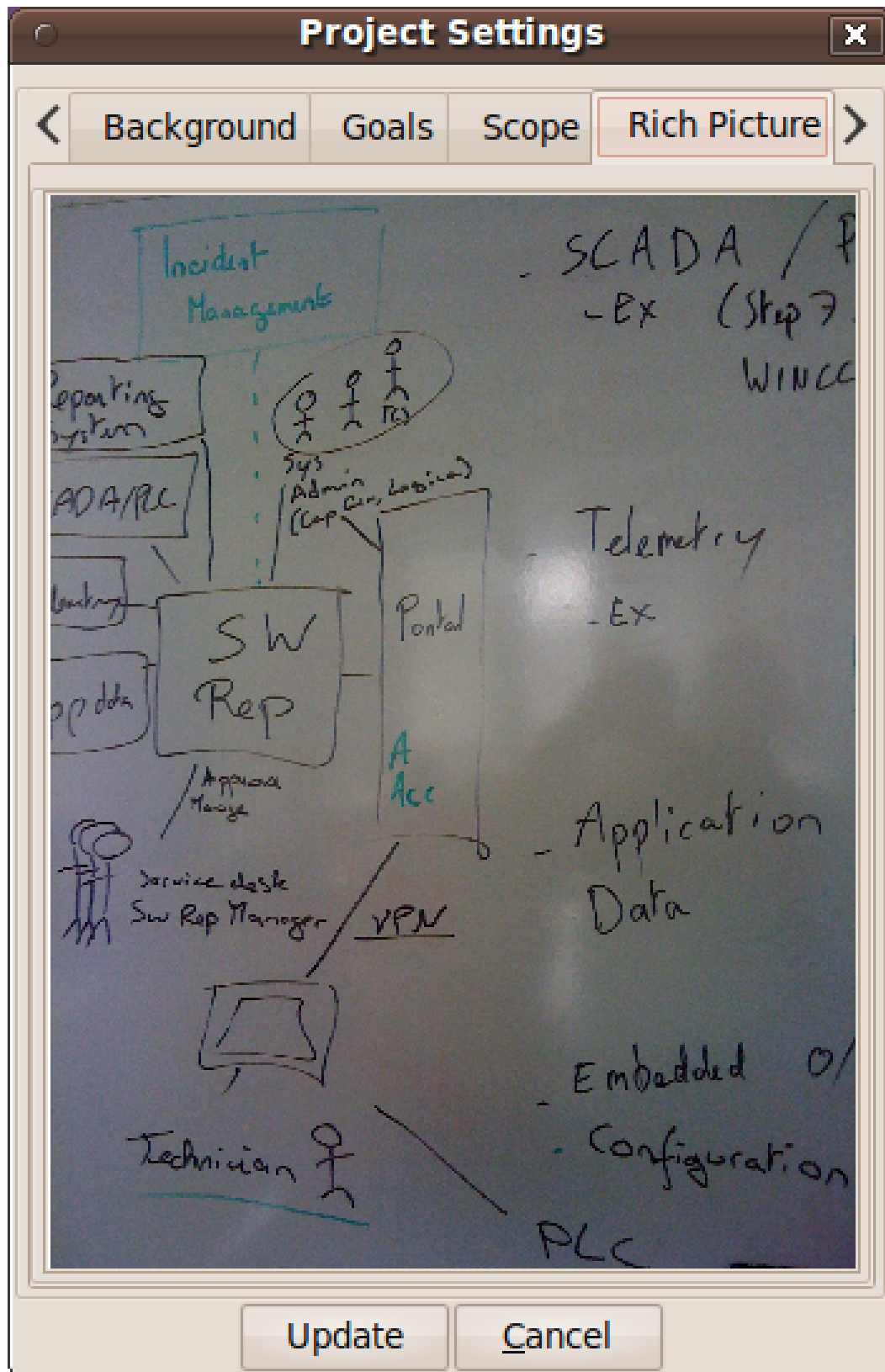


Figure 5: Project Settings notebook

**Edit environment**

Name  
Planned

Short Code  
PLAN

Environment

Duplication properties  
Override ☒ ▼  
Maximise ☐

Description  
Planned changes to sites and equipment. In-hours work.  
Plant modification to overhaul a piece of equipment.

Update Close

Figure 6: Environment Dialog

- Enter the name of the environment, a short code, and a description. The short-code is used to prefix requirement ids associated with an environment.
- If this environment is to be a composite environment, i.e. encompass artifacts of other environments, then right click on the environment list, select Add from the speed menu, and select the environment/s to add.
- It is possible artifact may appear in multiple environments within a composite environment. It is, therefore, necessary to set duplication properties for composite environments. If the maximise radio button is selected, then the maximal values associated with that artifact will be adopted. This may be the highest likelihood value for a threat, or the highest security property values for an asset. If the override radio button is selected, then CAIRIS will ensure that the artifact properties are used for the overriding environment.

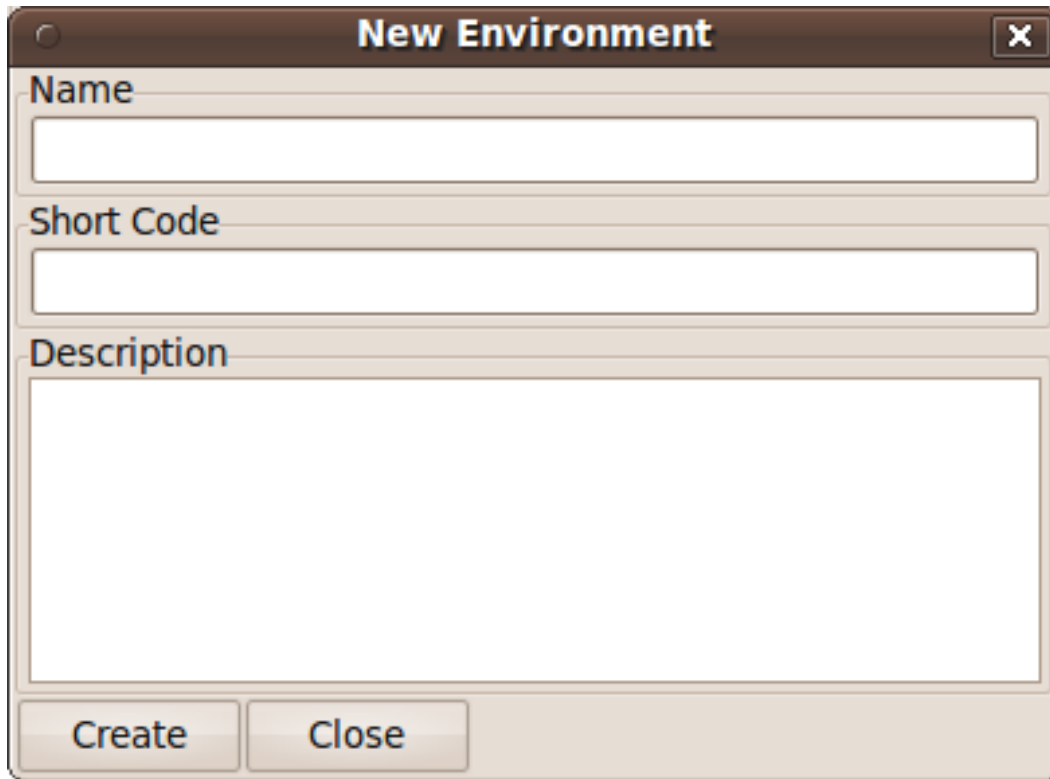
A screenshot of a software dialog box titled "New Environment". The dialog has a standard window frame with a title bar and a close button (X) in the top right corner. Inside the dialog, there are three input fields: "Name" (a single-line text box), "Short Code" (a single-line text box), and "Description" (a multi-line text area). At the bottom of the dialog, there are two buttons: "Create" and "Close".

Figure 7: New Environment Dialog

## 10.2 On-the-fly environment creation

Most artifacts in CAIRIS are situated in one or more environments. When creating or updating an artifact, it is usually possible to create a new environment on the fly by right-clicking on the environment list box in the artifact dialog and selecting the New button. This opens the New Environment dialog box (figure fig:NewEnvironmentDialog (Figure 7). In this dialog, an environment name, short code and description can be entered. When the create button is selected, a new environment is added to the CAIRIS database, and added to the environment list for the artifact.

## 10.3 Environmental attribute inheritance

An artifact may be situated in one or more environments, but the differences between these environments may be slight. To reflect this, it is possible for an artifact to inherit properties from another environment. To do this, right-click on the artifact's environment list box and select the Inherit Environment option. When prompted, select the environment to inherit from, followed by the environment to situated the artifact in. In most cases, the properties of the inherited environment will be duplicated in this newly situated environment. In the case of goals and obstacles, only the immediate refinement associations are retained when

inheriting properties from an environment.

## 11 Assets

### 11.1 Overview

Assets are tangible objects of value to stakeholders. By defining an asset in CAIRIS, we implicitly state that this needs to be secured in light of risks which subsequently get defined.

Assets are situated in one or more environments. Security properties are associated with each asset for every environment it can be found in. These security properties are Confidentiality, Integrity, Availability, and Accountability. Each of these properties is associated with the value of None, Low, Medium, or High. The meaning of each of these values can be defined in CAIRIS from the Asset Values dialog; this is available via the Options/Asset values menu.

### 11.2 Adding, updating, and deleting an asset

- Click on the Asset toolbar button to open the Assets dialog box, and click on the Add button to open the Asset dialog box.
- Enter the name of the environment, a short code, description, and significance. The short-code is used to prefix requirement ids associated with an environment.
- If this asset is deemed critical, click on the Criticality tab, and click on the Critical Asset check-box. A rationale for declaring this asset critical should also be added. By declaring an asset critical, any risk which either threatens or exploits this asset will be maximised until the mitigations render the likelihood of the threat or the severity of the vulnerability inert.
- Right click on the environment window to bring up the environment speed menu. Select the add option and, from the Add environment window, select an environment to situate the asset in. This will add the new environment to the environment list.
- After ensuring the environment is selected in the environment window, add the security properties to this asset for this environment. Security properties are added by selecting the Properties tab, right clicking on the properties list and selecting Add to open the Add Security Properties window. From this window, a security property and its value can be added.
- Click on the Create button to add the new asset.
- Existing assets can be modified by double clicking on the asset in the Assets dialog box, making the necessary changes, and clicking on the Update button.
- To delete an asset, select the asset to delete in the Assets dialog box, and select the Delete button. If any artifacts are dependent on this asset then a dialog box stating these dependencies are displayed. The user has the option of selecting Yes to remove the asset dependencies and the asset itself, or No to cancel the deletion.



**Edit asset**

Name  
PLC Software

Short Code  
PLCS

Type  
Software

Description Significance

A binary project file containing hardware configuration data, module parameterisation data, program source, and associated meta-data.

Environment  
Planned  
Unplanned

Properties Associations

Property	Value
Integrity	High
Availability	High
Accountability	Medium

Update Close

Figure 8: Asset Dialog

### 11.3 Asset modelling

Understanding how assets can be associated with each other is a useful means of identifying where the weak links in a prospective architecture might be. CAIRIS supports the association of assets, inconsistency checking between associated assets, and visualisation of asset models.

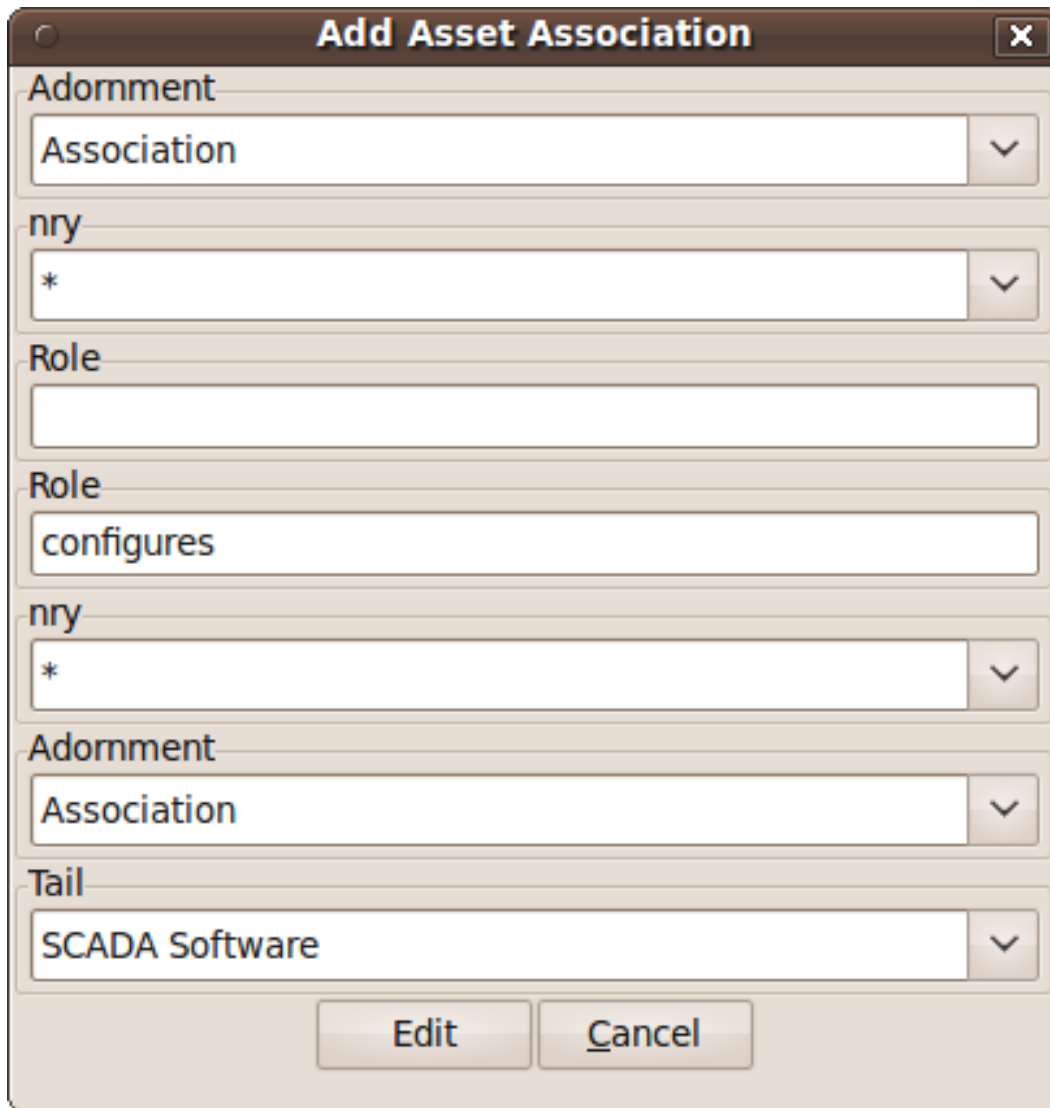
The CAIRIS asset model is based on UML class models. Asset models can be viewed for each defined environment. As well as explicitly defined asset associations, asset models will also contain associations implicitly defined. For example, if a task has been defined, and this task concerns within an environment contain one or more assets, then the participating persona will be displayed as an actor, and an association between this actor and the asset will be displayed. Additionally, if concern associations have been defined between goals and assets and/or associations then zooming into the model will display these concerns; the concerns are displayed as blue comment elements.

#### Adding an asset association

- If creating or updating an asset, an association between that asset and another asset can be made by clicking on the Associations tab in the Asset Dialog and, from the right-click speed menu, selecting Add to open the Add Asset Dialog (figure fig:AddAssetAssociation (Figure 9)).
- From the Add Asset Dialog, set the adornments for the head and tail end of the association. Possible adornment options are Inheritance, Association, Aggregation, and Composition; the semantics for these adornments are based on UML.
- Set the multiplicity (nry) for the head and tail ends of the association. Possible multiplicity options are 1, , and 1...
- Optional role names can also be set at the head or tail end of the association.
- Select the Create (or Edit if modifying an existing association) will add the association to the Asset Dialog. The association will not be added to the database until the asset itself is created or modified.
- Asset associations can also be added by selecting the Asset Associations tool-bar button. Clicking this button opens the Asset Associations dialog, where new associations can be created or existing associations can be modified or removed. The dialog for modifying associations is identical to the Asset Association dialog in figure [fig:AddAssetAssociation], with the addition of a combo box for selecting the environment to situate the association in.
- If an asset is associated with an asset with one or more security properties of a lower value, then an Asset Inconsistency dialog (figure fig:AssetInconsistency (Figure 10)) displayed, warning about the details of the inconsistency.

#### Viewing Asset models

Asset models can be viewed by clicking on the Asset Model toolbar button, and selecting the environment to view the environment for.



The dialog box is titled "Add Asset Association" and contains several input fields and buttons. The fields are arranged in a vertical stack, each with a label and a text input area with a dropdown arrow on the right. The labels are: "Adornment", "nry", "Role", "Role", "nry", "Adornment", and "Tail". The input values are: "Association", "\*", an empty field, "configures", "\*", "Association", and "SCADA Software". At the bottom of the dialog are two buttons: "Edit" and "Cancel".

Field Label	Input Value
Adornment	Association
nry	*
Role	
Role	configures
nry	*
Adornment	Association
Tail	SCADA Software

Buttons: Edit, Cancel

Figure 9: Add Asset Association Dialog

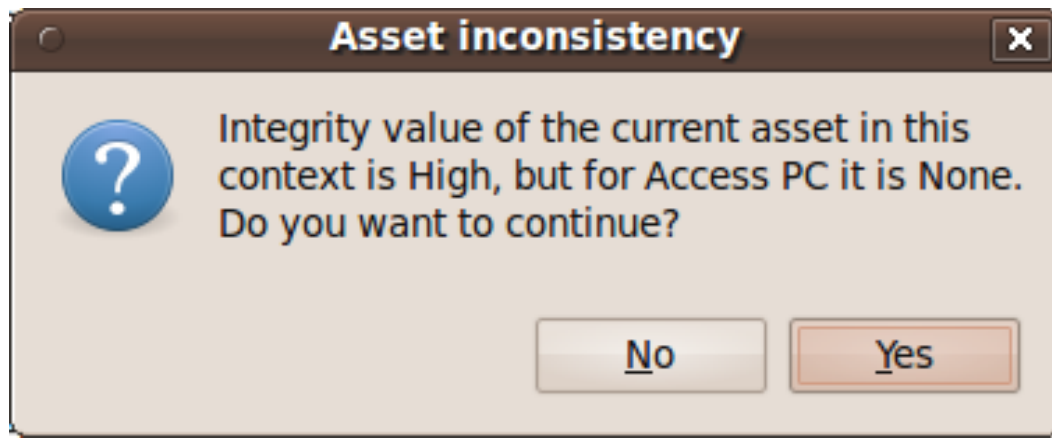


Figure 10: Asset Inconsistency warning

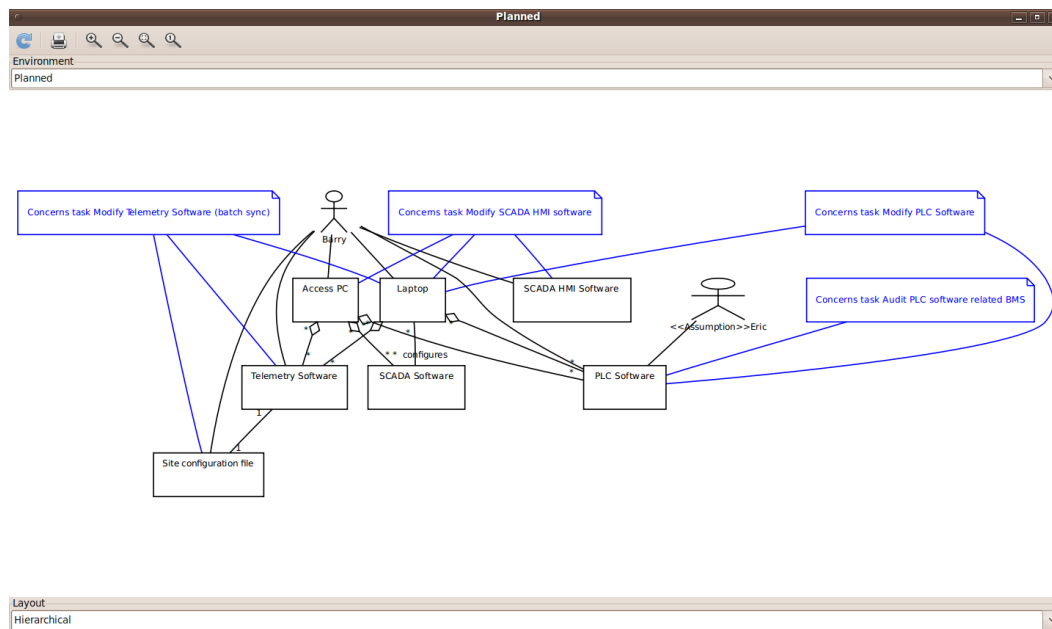


Figure 11: Asset Model

By changing the environment name in the environment combo box, the asset model for a different environment can be viewed. The layout of the model can also be replaced by selecting a layout option in the Layout combo box at the foot of the model viewer window.

By clicking on a model element, information about that artifact can be viewed.

## 12 Roles and Personas

### 12.1 Roles

Roles represent the abstract classes representing human agents; these also encapsulate behaviours and responsibilities. CAIRIS supports 2 types of role: stakeholder and attacker. Stakeholder roles represent human agents the system needs to be directly, or indirectly designed for. Attackers are human agents the system should not be designed for.

### 12.2 Adding, updating, and deleting a role

- Click on the Role toolbar button to open the Roles dialog box, and click on the Add button to open the Role dialog box.
- Enter a role name and description, and select the role type.
- Click on the Update button to Add the new role to the CAIRIS database.
- As responses and countermeasures are assigned to roles, the Role dialog is automatically updated to reflect these new dependencies. These dependencies can not be modified from the Role dialog.
- Existing roles can be modified by double clicking on the role in the Roles dialog box, making the necessary changes, and clicking on the Update button.
- To delete a role, select the role to delete in the Roles dialog box, and select the Delete button. If any artifacts are dependent on this role then a dialog box stating these dependencies are displayed. The user has the option of selecting Yes to remove the role dependencies and the role itself, or No to cancel the deletion.

### 12.3 Responsibility modelling

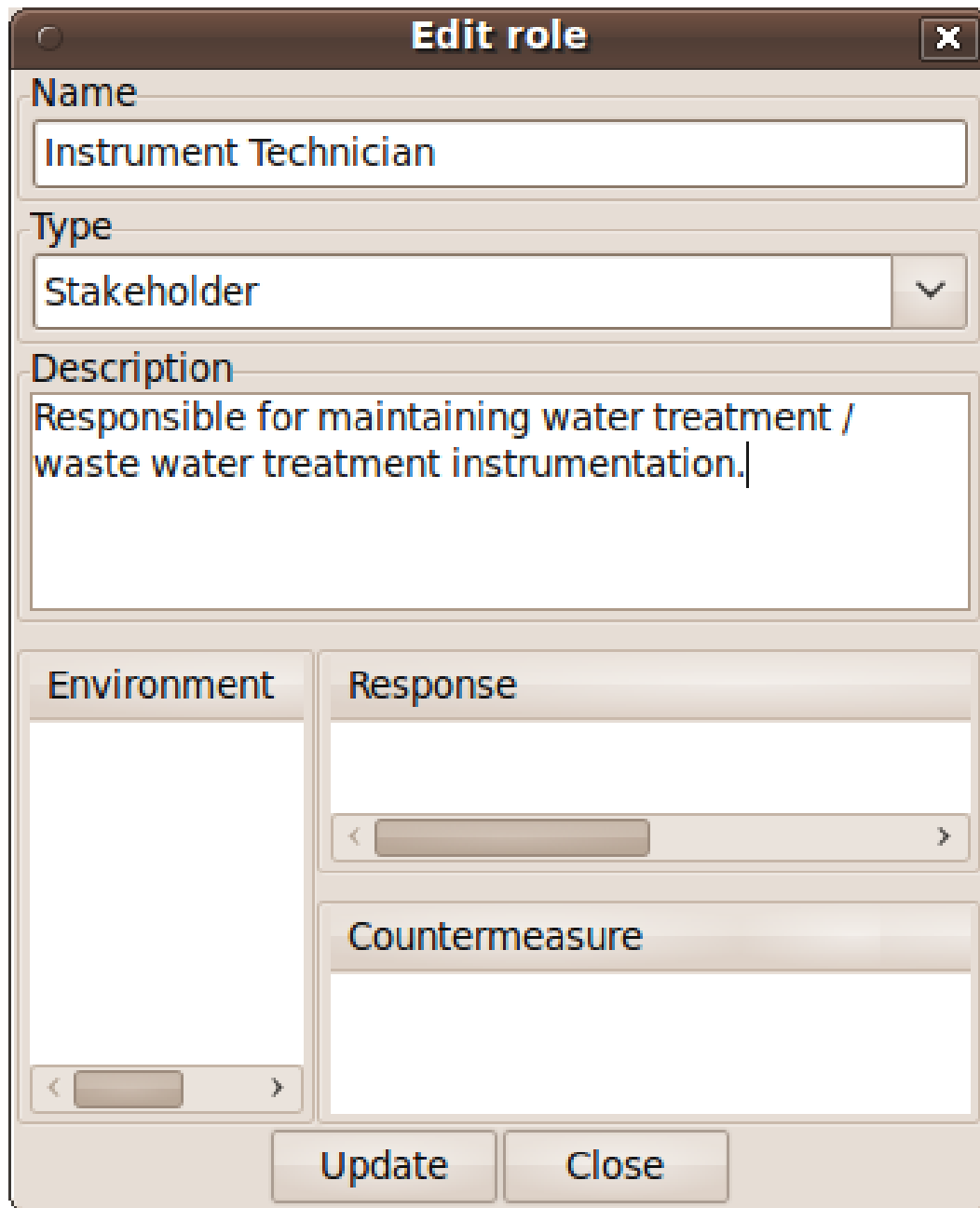
Responsibility models can be viewed by clicking on the View Responsibility Model toolbar button, and selecting the environment to view the environment for.

By changing the environment name in the environment combo box, the responsibility model for a different environment can be viewed. The layout of the model can also be replaced by selecting a layout option in the Layout combo box at the foot of the model viewer window.

By clicking on a model element, information about that artifact can be viewed.

### 12.4 Personas

Personas are specifications of archetypical users that the system needs to directly or indirectly cater for. The system needs to be specified for Primary Personas, but Secondary



The image shows a software dialog box titled "Edit role" with a close button (X) in the top right corner. The dialog is organized into several sections. The "Name" section contains a text input field with the value "Instrument Technician". The "Type" section features a dropdown menu currently set to "Stakeholder". The "Description" section is a larger text area containing the text "Responsible for maintaining water treatment / waste water treatment instrumentation." Below these sections, there are two main areas: "Environment" on the left and "Response" on the right. The "Environment" area has a large empty text box and a scrollbar at the bottom. The "Response" area contains a text box, a scrollbar, and a "Countermeasure" section with another empty text box. At the bottom of the dialog are two buttons: "Update" and "Close".

**Edit role** [X]

**Name**

Instrument Technician

**Type**

Stakeholder

**Description**

Responsible for maintaining water treatment /  
waste water treatment instrumentation.

**Environment**

**Response**

**Countermeasure**

Update Close

Figure 12: Role Dialog

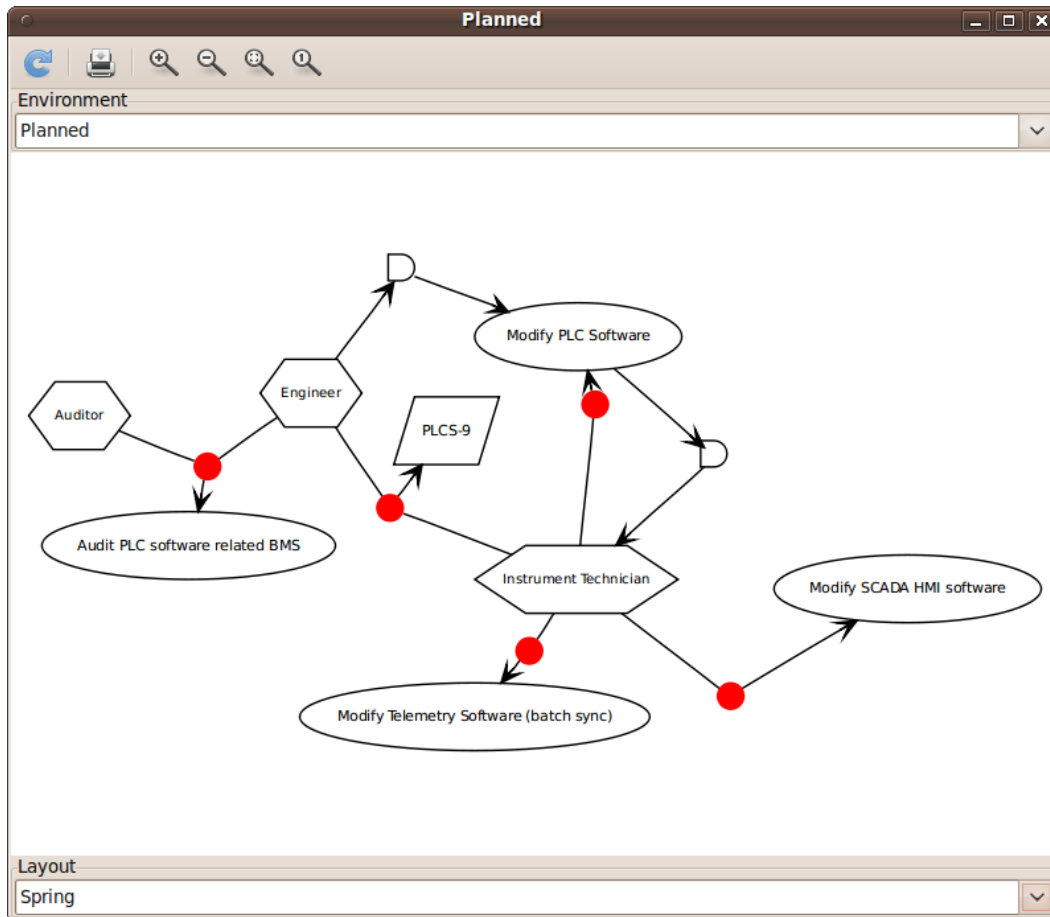


Figure 13: Responsibility Model

Personas cannot be ignored as their thoughts or concerns provide insight into potential usability problems.

### Adding, updating, or deleting a persona

- Click on the Persona toolbar button to open the Personas dialog box, and click on the Add button to open the Persona dialog box.
- Enter a persona name and select the persona type.
- If the persona is not derived from empirical data, then select the Assumption Persona check-box. Ticking this box has the effect of pre-fixing the persona name with the << assumption >> stereotype in any models where the persona is present.
- Click on the Activities tab and enter the activities carried out by the personas.

**Edit persona** [X]

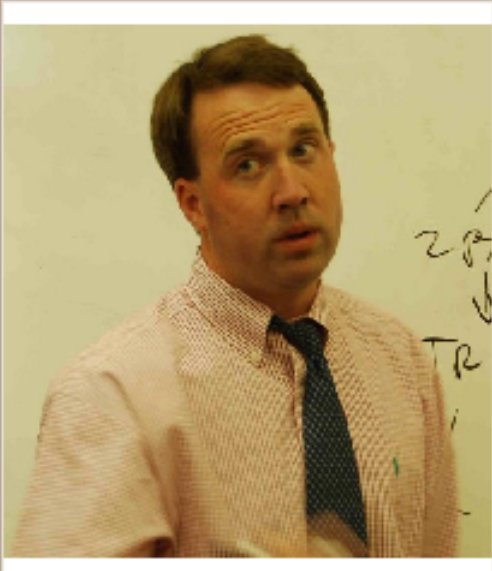
Name  
Alan

Type  
Secondary

Assumption Persona  
☐

< Activities Attitudes >

Because much of his work involves working with electrical engineers, Alan understands the importance of documentation as a means of communication. Therefore, he tries to make sure that when a project is handed over, an instrument tech has everything he needs to



Environment  
Planned  
Unplanned

Summary Narrative  
Direct/Indirect Persona  
☒

Role  
Engineer

< [ ] >

Update Close

Figure 14: Persona Dialog



- Click on the Attitudes tab and enter the attitudes held by the persona, with respect to the problem domain the system will be situated in.
- Click on the Aptitudes tab and enter the persona's aptitudes, with respect to the problem domain the system will be situated in.
- Click on the Motivations tab and enter the persona's personal motivations.
- Click on the Skills tab and enter the persona's skill-set, with respect to the problem domain the system will be situated in.
- If you have decided to personalise the persona with a picture, this can be added by right clicking on photo box next to the persona properties notebook, to bring up the Load Image option from the speed menu, and selecting Load Image. Please note that the image itself is NOT imported into the database, only the file path to the picture.
- If you have decided to personalise your persona with a picture, this can be added by right clicking on the photo
- Right click on the environment window to bring up the environment speed menu. Select the add option and, from the Add environment window, select an environment to situate the persona in. This will add the new environment to the environment list.
- After ensuring the environment is selected in the environment window, click on the Summary tab. Select the Direct/Indirect Persona check-box if the persona is a direct stakeholder with respect to the system being defined, and add roles fulfilled by the persona in the Roles list-box. These roles can be added or deleted by right clicking on the roles box to bring up the speed menu.
- Click on the Narrative tab and enter a narrative describing the persona's relationship with the problem domain or prospective system within the environment, and any environment specific concerns he or she might have.
- Click on the Create button to add the new persona.
- Existing personas can be modified by double clicking on the persona in the Personas dialog box, making the necessary changes, and clicking on the Update button.
- To delete a persona, select the persona to delete in the Personas dialog box, and select the Delete button. If any artifacts are dependent on this persona then a dialog box stating these dependencies are displayed. The user has the option of selecting Yes to remove the persona dependencies and the persona itself, or No to cancel the deletion.

### Recording persona assumptions

- From the Options/External Document directory, click on the Add button and add information about the source of any assumptions external to CAIRIS. An example of such an *External Document* might be an interview transcript. Alternatively, if assumptions are purely based on your own thoughts and feelings then an External Document can be created to make this explicit.
- Open up the Persona dialog for the persona you want to add a characteristic to, and right click in the behavioural variable folder (e.g. Activities) you wish to add a Characteristic to.

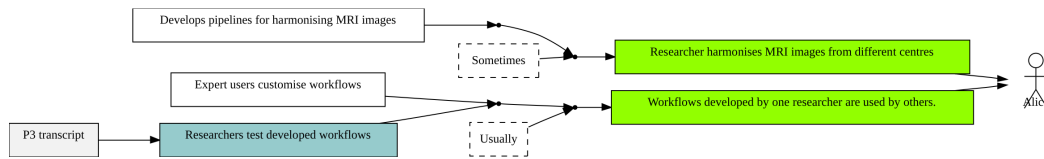


Figure 15: Assumption Persona model

- From the Persona Characteristics dialog box, click on Add to add a new characteristic.
- From the General folder, add a description of the characteristic and a *Model Qualifier*; this word describes your confidence in the validity of the characteristic. Possible qualifiers might include *always*, *usually*, or *perhaps*.
- Click on the Grounds tab to open the list of Grounds for this characteristic. The grounds are evidence which support the validity of the characteristic. Right click in the Reference box, and select Add to add a Document Reference. Select the concept type for this evidence and the name of a pre-existing concept or document reference for this grounds. If one doesn't already exist, then select any artifact and, from the Reference combo box, select [New artifact reference] (for a document reference) or [New concept reference] (for a reference to an existing model object). In both cases, a dialogue box will appear allowing you to enter a short description of the grounds proposition, together with more detailed rationale. Clicking on Ok will add the new document or concept reference, and add this to the grounds list.
- Click on the Warrant tab to open the list of Warrants for this characteristic. The warrants are inference rules which links the grounds to the characteristic. The procedure for adding warrants is identical to the process for adding grounds. After adding a warrant, however, a Backing entry for the warrant is automatically added.
- If you wish to add a Rebuttal – a counterargument for the characteristic – then click on the Rebuttals tab and add a rebuttal using the same procedure for Grounds and Warrants.
- Click on the Create button to create the new characteristic.
- Existing characteristics can be modified by double clicking on the characteristics in the Persona Characteristic dialog box, making the necessary changes, and clicking on the Edit button.

## 13 Tasks

### 13.1 Overview

Tasks model the work carried out by one or more personas. This work is described in environment-specific narrative scenarios, which illustrate how the system is used to augment the work activity.

**Edit Task**

Name  
Modify PLC Software

Assumption Task  
☐

Objective  
Modify the PLC software in order to maintain plant operation.

Environment  
Planned  
Unplanned

Summary Narrative Concern Associations

Dependencies  
Barry has looked at the code before hand, so is aware of what amendments need to made, and his aware of the PLC he needs to modify.  
A job has been raised on the planned worksystem and picked up.

Persona	Duration	Frequency	Demands	Goals
Barry	Hours or longer	Monthly or less	High	High

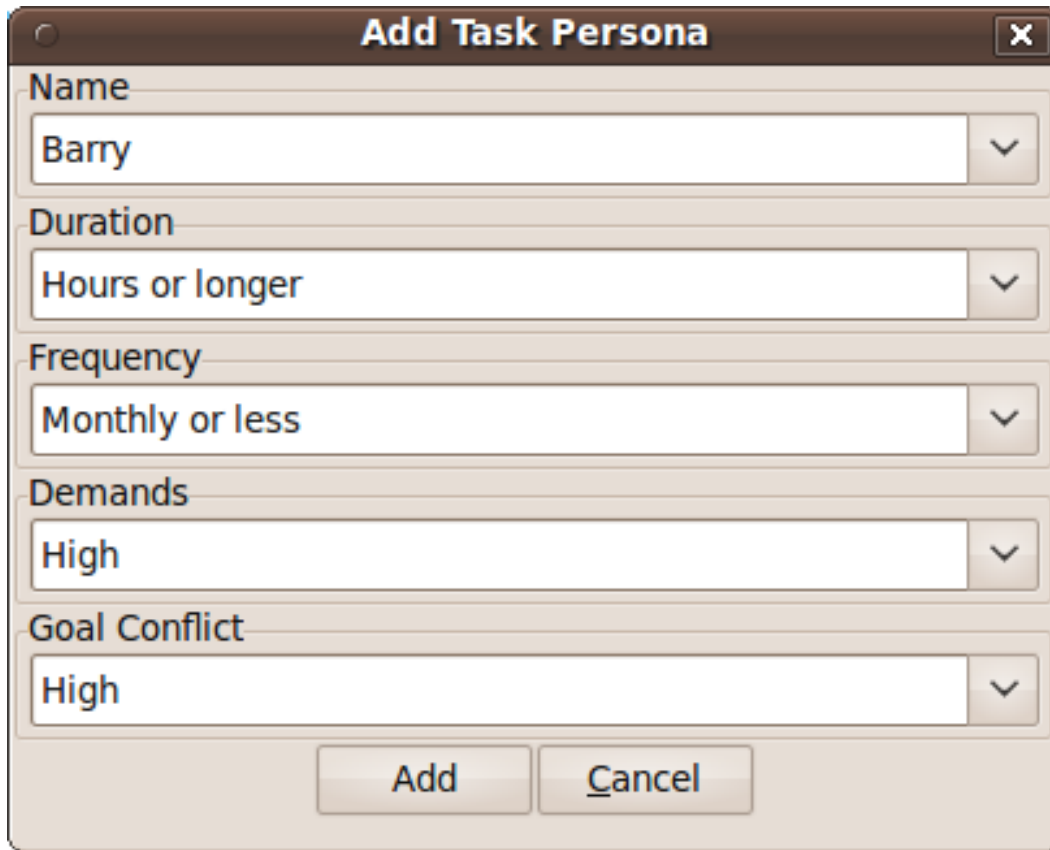
Concerns  
Laptop  
PLC Software

Update Close

Figure 16: Task Dialog

### 13.2 Adding, updating, or deleting a task

- Click on the Task toolbar button to open the Tasks dialog box, and click on the Add button to open the Task dialog box.
- Enter a task name, and the objective of carrying out the task.
- If the task is not derived from empirical data, then select the Assumption Task check-box. Ticking this box has the effect of pre-fixing the task name with an << assumption >> stereotype in any models where the task is present.
- Right click on the environment window to bring up the environment speed menu. Select the add option and, from the Add environment window, select an environment to situate the persona in. This will add the new environment to the environment list.



The image shows a dialog box titled "Add Task Persona". It contains five dropdown menus, each with a label and a selection box. The first dropdown is labeled "Name" and has "Barry" selected. The second is labeled "Duration" and has "Hours or longer" selected. The third is labeled "Frequency" and has "Monthly or less" selected. The fourth is labeled "Demands" and has "High" selected. The fifth is labeled "Goal Conflict" and has "High" selected. At the bottom of the dialog are two buttons: "Add" and "Cancel".

Field	Value
Name	Barry
Duration	Hours or longer
Frequency	Monthly or less
Demands	High
Goal Conflict	High

Figure 17: Add Task Persona Dialog

- After ensuring the environment is selected in the environment window, click on the Summary tab. In the Summary page, enter any dependencies needing to hold before this task can take place.
- Right click on the persona list box and select Add from the speed menu to associate a persona with this task. In the Add Task Persona dialog box (figure fig:AddTaskPersona (Figure 17)) select the person, the task duration (seconds, minutes, hours or longer), frequency (hourly or more, daily-weekly, monthly or less), demands (none, low, medium, high), and goal conflict (none, low, medium, high). The values for low, medium, and high should be agreed with participants before hand.
- If any aspect of the task concerns one or more assets, then these can be added to the concern list. Adding an asset concern causes a concern comment to be associated to the asset in the asset model. If the task concerns an association between assets, the association can be added by clicking on the Concern Association tab and adding the source and target assets and association multiplicity to the concern association list. In the asset model, this association is displayed and a concern comment is associated to each asset in the association.

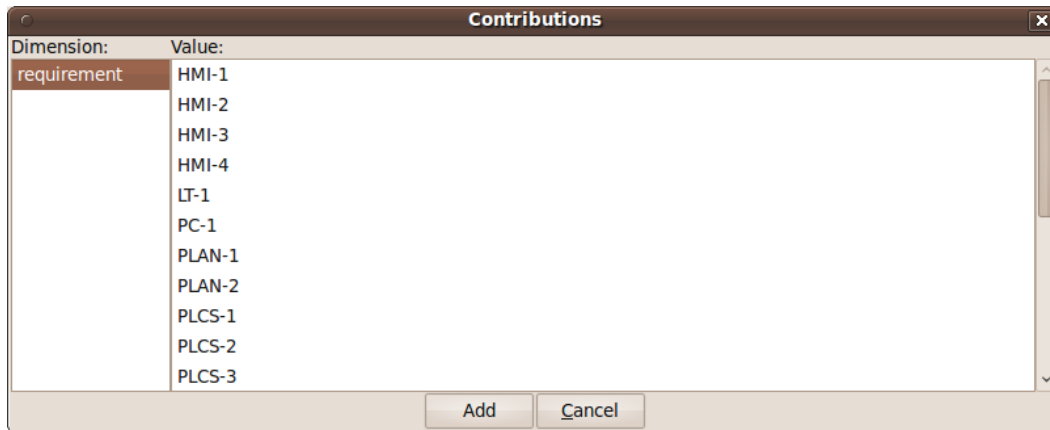


Figure 18: Traceability Editor

- Right click on the Narrative tab and enter the task scenario in the text box. This narrative should describe how the persona (or personas) carry out the task to achieve the pre-defined objective.
- Click on the Create button to add the new task.
- Existing tasks can be modified by double clicking on the task in the Tasks dialog box, making the necessary changes, and clicking on the Update button.
- To delete a task, select the task to delete in the Tasks dialog box, and select the Delete button. If any artifacts are dependent on this task then a dialog box stating these dependencies are displayed. The user has the option of selecting Yes to remove the task dependencies and the task itself, or No to cancel the deletion.

### 13.3 Task traceability

Tasks can be manually traced to certain artifacts via the Tasks dialog. A task may contribute to an asset or a vulnerability, or be supported by requirement. To add a traceability link, right click on the task name, and select Supported By or Contributes to. This opens the Traceability Editor (figure fig:TraceabilityEditor (Figure 18)). From this editor, select the object on the right hand side of the editor to trace to and click the Add button to add this link.

Manual traceability links can be removed by selecting the View/Traceability menu option, to open the Traceability Relations dialog. In this dialog box, manual traceability relations be removed from specific environments.

### 13.4 Visualising tasks

Task models can be viewed by clicking on the Task Model toolbar button, and selecting the environment to view the environment for.

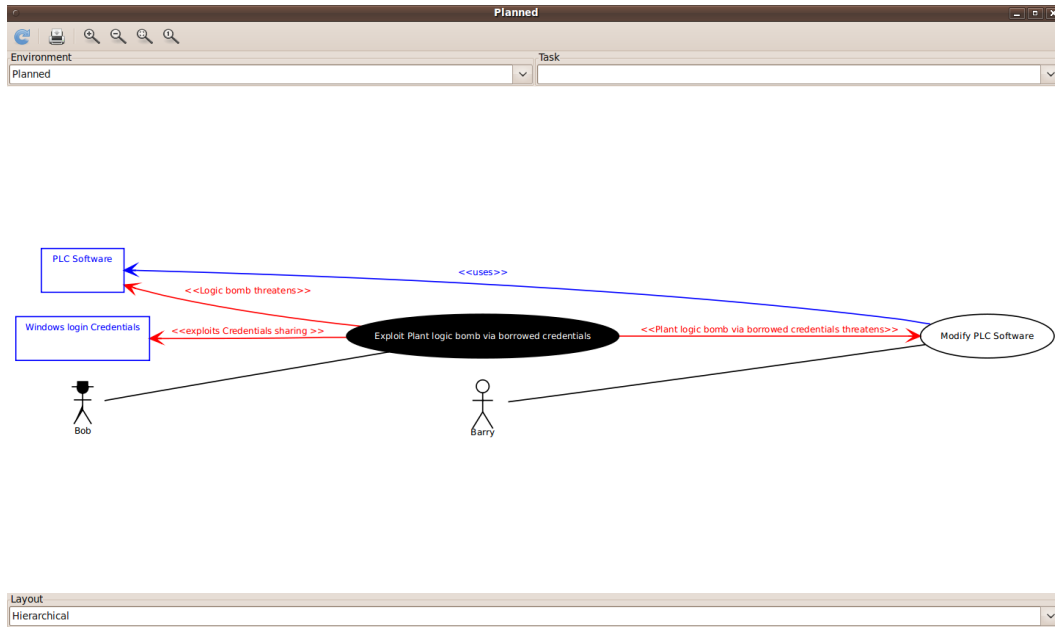


Figure 19: Task Model

By changing the environment name in the environment combo box, the task model for a different environment can be viewed. The layout of the model can also be replaced by selecting a layout option in the Layout combo box at the foot of the model viewer window.

By clicking on a model element, information about that artifact can be viewed.

## 14 Domain Properties

Domain Properties are descriptive properties about the statement world. Domain Properties may be either hypothesis or invariants.

### 14.1 Adding, updating, and deleting a domain property

- Click on the Domain Properties toolbar button to open the Domain Properties dialog box, and click on the Add button to open the Domain Property dialog box.
- Enter a domain property name, description, and select the type of domain property from the type combo box.
- Click on the Create button to add the new domain property.
- Existing domain properties can be modified by double clicking on the domain property in the Domain Properties dialog box, making the necessary changes, and clicking on the Update button.

**Edit Domain Property**

**Name**  
Software Tool Installation

**Type**  
Hypothesis

**Description**  
Software Tools for downloading software to PLCs, outstations or panels is correctly installed on laptops and access PCs used by technicians.

Update Close

Figure 20: Domain Property Dialog

## 15 Goals, Requirements and Obstacles

In CAIRIS, a requirements specification is analogous to a safety case. In a safety case, a system is only considered safe if its safety goals have been satisfied. In a similar manner, requirements are leaf nodes in a goal tree and satisfying stakeholder needs is only possible if the high-level goals – stipulated by stakeholders – can be satisfied.

We define goals as prescriptive statements of system intent that are achievable by one or more agents. Goals can be refined to requirements, which are achievable by only agent. Goals and requirements may also be operationalised as tasks. Alternatively, we may decide to specify tasks and ask what goals or requirements need to hold in order that a given task can be completed successfully.

To satisfy a goal, one or more sub-goals may need to be satisfied; satisfaction may require satisfying a conjunction of sub-goals, i.e. several AND goals, or a disjunction of sub-goals, i.e. several OR goals.

Goals or requirements may be obstructed by obstacles, which are conditions representing undesired behaviour; these prevent an associated goal from being achieved. By progressively refining obstacles, we can obtain the origin of some undesired behaviour; this may be reflected as a vulnerability or a threat, and contribute to risk analysis.

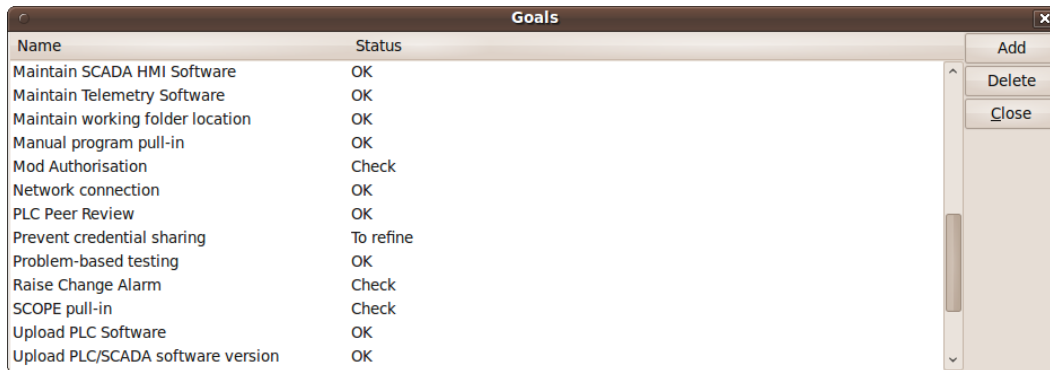


Figure 21: Goals Dialog

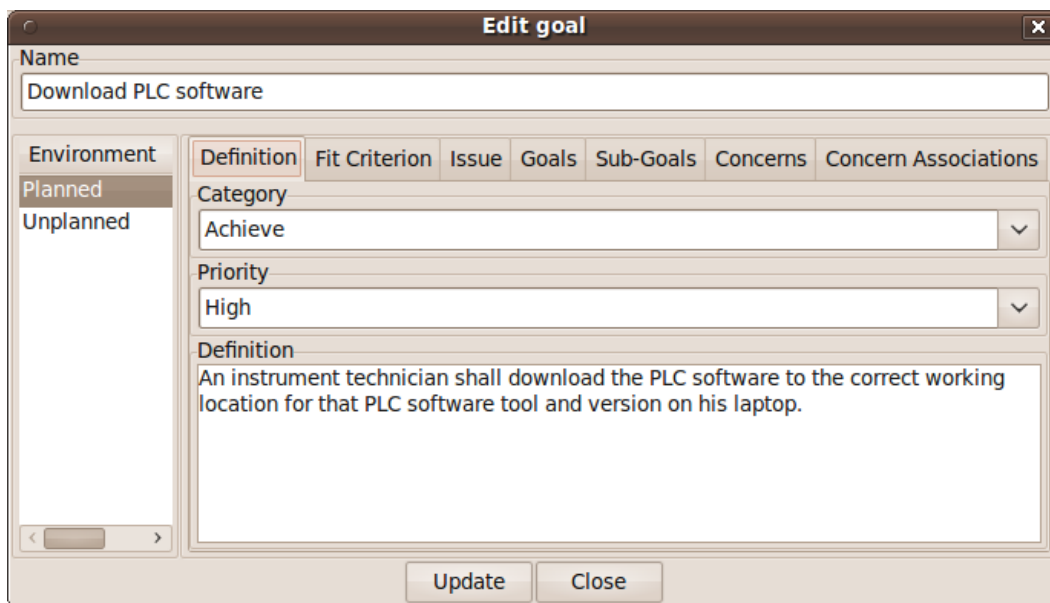


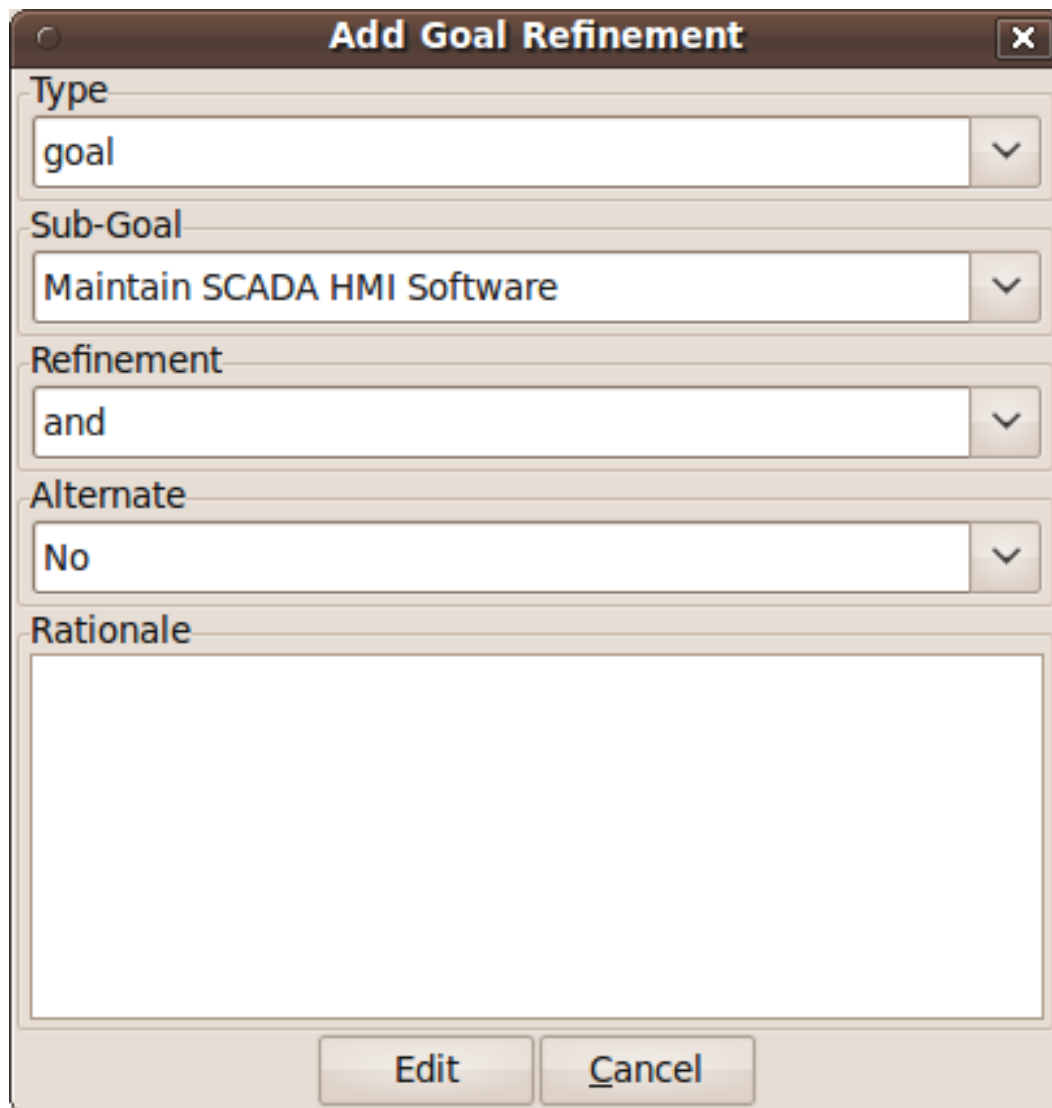
Figure 22: Goal Dialog

### 15.1 Adding, updating, and deleting a goal

- Click on the Goal toolbar button to open the Goals dialog box. As fig:GoalsDialog (Figure 21) illustrates, next to goal name is the current *status* for the goal. If a goal is defined as OK, then this goal is refined by a requirement, or by one or more goals. Goals with the status *to refine* have yet to be refined or operationalised. Goals with the status *Check* have been refined by one or more obstacle, and these should be examined to find a root threat or vulnerability.



- Click on the Add button to open the Goal dialog box, and enter the name of the goal.
- Right click on the environment window to bring up the environment speed menu. Select the add option and, from the Add environment window, select an environment to situate the goal in. This will add the new environment to the environment list.
- In the Definition page, enter the goal definition, and select the goal category and priority. Possible goal categories are: Achieve, Maintain, Avoid, Improve, Increase, Maximise, and Minimise. Possible priority values are Low, Medium, and High.
- Click on the Fit Criterion tab, and enter the criteria which must hold for the goal to be satisfied.
- Click on the Issue tab and enter any issues or comments relating to this goal.
- If this goal refines a parent goal, click on the Goals tab, right-click on Goal refinement list, and select Add to open the Add Goal Refinement Dialog (figure fig:AddGoalRefinement (Figure 23)). In this dialog, select the Goal from the Type combo box, and select the Sub-goal, refinement type, and an Alternate value. Possible refinement types are: and, or, conflict, responsible, obstruct, and resolve. The alternative value (Yes or No) indicates whether or not this goal affords a goal-tree for an alternate possibility for satisfying the parent goal. It is also possible to enter a rationale for this goal refinement in the refinement text box. Clicking on Add will add the refinement association to memory, but this will not be committed to the database until the goal is added or updated.
- If this goal refines to sub-goals already specified, Click on the Sub-Goals tab and add a goal refinement association as described in the previous step. A goal may refine to artifacts other than goals, specifically tasks, requirements, obstacles, and domain properties.
- Goal refinements can also be specified independently of goal creation or modification via the Goal Associations tool-bar button.
- If any aspect of the goal concerns one or more assets, then these can be added by clicking on the Concerns add and adding the asset/s to the concern list. Adding an asset concern causes a concern comment to be associated to the asset in the asset model. If the goal concerns an association between assets, the association can be added by clicking on the Concern Association tab and adding the source and target assets and association multiplicity to the concern association list. In the asset model, this association is displayed and a concern comment is associated to each asset in the association.
- Click on the Create button to add the new goal.
- Existing goals can be modified by double clicking on the goal in the Goals dialog box, making the necessary changes, and clicking on the Update button.
- To delete a goal, select the goal to delete in the Goals dialog box, and select the Delete button. If any artifacts are dependent on this goal then a dialog box stating these dependencies are displayed. The user has the option of selecting Yes to remove the goal dependencies and the goal itself, or No to cancel the deletion.



The image shows a software dialog box titled "Add Goal Refinement". It has a standard window title bar with a close button (X) in the top right corner. The dialog is divided into several sections, each with a label and a corresponding input field or list:

- Type:** A dropdown menu with "goal" selected.
- Sub-Goal:** A dropdown menu with "Maintain SCADA HMI Software" selected.
- Refinement:** A dropdown menu with "and" selected.
- Alternate:** A dropdown menu with "No" selected.
- Rationale:** A large, empty text area for providing a rationale.

At the bottom of the dialog, there are two buttons: "Edit" and "Cancel".

Figure 23: Add Goal Refinement Dialog

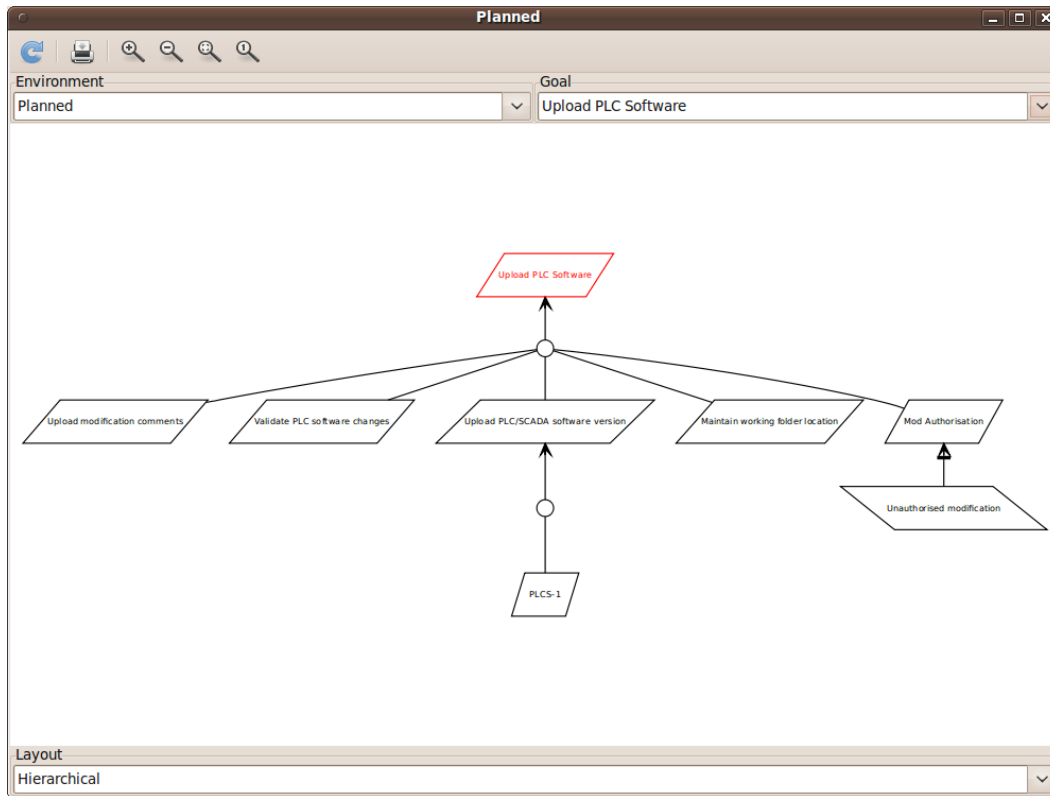


Figure 24: Goal Model

## 15.2 Goal Modelling

Goal models can be viewed by clicking on the Goal Model toolbar button, and selecting the environment to view the environment for.

By changing the environment name in the environment combo box, the goal model for a different environment can be viewed. The layout of the model can also be replaced by selecting a layout option in the Layout combo box at the foot of the model viewer window.

By clicking on a model element, information about that artifact can be viewed.

Goal models can also be filtered by goal. Applying a filter causes the selected goal to be displayed as the root goal. Consequently, goals are only displayed if they are direct or indirect leafs of the filtered goal.

Goals can also be refined from the goal model, albeit only for the environment being modified. To refine a goal, right-click on the goal in the model viewer, and select And-Goal, or Or-Goal based on the refinement desired. An simplified version of the Add Goal dialog box is displayed and, when all the necessary information has been added, a new goal will be added to the database, complete with the desired refinement. Please note, the model view needs to be refreshed to view the goal. Goals may only be refined to other goals in the model viewer; for anything more elaborate, the usual goal refinement association procedure needs to be followed.

**Edit obstacle**

Name  
Credential sharing

Environment  
Planned  
Unplanned

Definition Goals Sub-Goals Concerns

Category  
Vulnerability

Definition  
Evidence that users are prepared to share their credentials with colleagues should the need arise.

Update Close

Figure 25: Obstacle Dialog

### 15.3 Adding, updating, and deleting an obstacle

- Click on the Obstacle toolbar button to open the Obstacles dialog box, and click on the Add button to open the Obstacle dialog box.
- Enter the name of the obstacle, and right click on the environment window to bring up the environment speed menu. Select the add option and, from the Add environment window, select an environment to situate the obstacle in. This will add the new environment to the environment list.
- In the Definition page, enter the obstacle definition, and select the obstacle category. Possible obstacle categories are: Confidentiality Threat, Integrity Threat, Availability Threat, Accountability Threat, Vulnerability, Duration, Frequency, Demands, and Goal Support.
- Like goals, obstacle refinements can be added via the Goals and Sub-Goals tabs.

- If any aspect of the obstacle concerns one or more assets, then these can be added by clicking on the Concerns add and adding the asset/s to the concern list. Adding an asset concern causes a concern comment to be associated to the asset in the asset model.
- Click on the Create button to add the new obstacle.
- Existing obstacles can be modified by double clicking on the obstacle in the Obstacles dialog box, making the necessary changes, and clicking on the Update button.
- To delete an obstacle, select the obstacle to delete in the Obstacles dialog box, and select the Delete button. If any artifacts are dependent on this obstacle then a dialog box stating these dependencies are displayed. The user has the option of selecting Yes to remove the obstacle dependencies and the obstacle itself, or No to cancel the deletion.

### 15.4 Obstacle Modelling

Obstacle models can be viewed by clicking on the Obstacle Model toolbar button, and selecting the environment to view the environment for.

In many ways, the obstacle model is very similar to the goal model. The main differences are goal filtering is not possible, only the obstacle tree is displayed, and obstacles refine to obstacles, as opposed to goals.

### 15.5 Adding, updating, and deleting requirements

Requirements are added and edited using the Requirements Editor in the main CAIRIS window. Each requirement is associated with an asset, or an environment. Requirements associated with assets may specify the asset, constrain the asset, or reference it in some way. Requirements associated with an environment are considered transient, and remain associated with an environment only until appropriate assets are identified.

- To add a requirement, press enter on an existing requirement, or click on the Add Requirement toolbar button. In both cases, a new requirement will appear beneath the row where the cursor is currently set.
- Enter the requirement description, rationale, fit criterion, and originator in the appropriate cells, select the priority (1,2, 3), and the requirement type (Functional, Data, Look and Feel, Usability, Performance, Operational, Maintainability, Portability, Security, Cultural and Political, and Legal).
- When the attributes have been entered, click on the Commit latest changes toolbar button to commit these requirement additions to the database.
- The order of requirements in the editor can be modified by left clicking on the row label and, while holding down the left mouse button, moving the row label to the appropriate position. When the mouse button is released, the requirement labels are re-ordered accordingly.

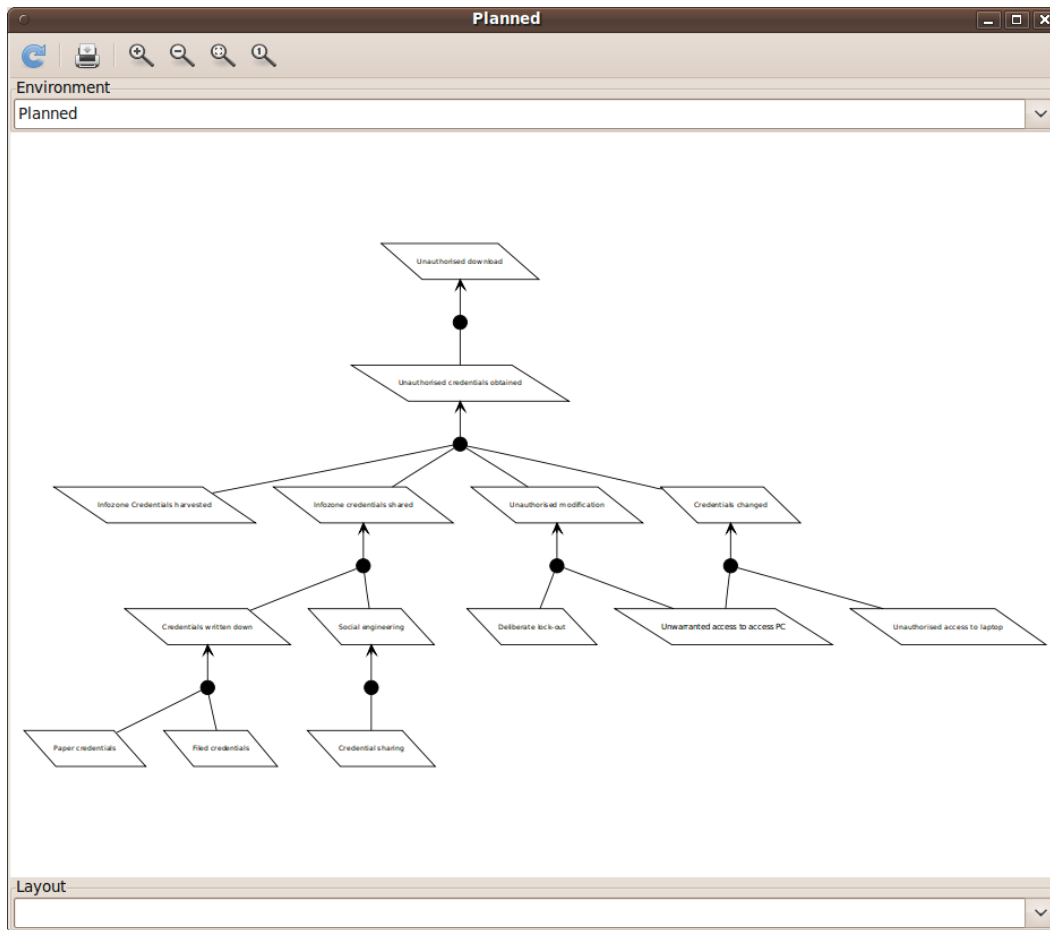


Figure 26: Obstacle Model

- By changing the asset in the Assets combo box, or the Environment in the Environments combo box, the editor will be reloaded with the requirement associated with the selected asset or environment. Please note, the Commit latest changes toolbar button should be clicked before changing the selected asset or environment, otherwise any in-situ requirement changes will be lost.
- A requirement can be deleting by moving the cursor to the row to be deleted, and clicking the Delete Requirements toolbar button. Deleting a requirement also has the effect of re-ordering the requirement labels.

## 15.6 Requirement history

Every time a requirement is modified, a new version of the requirement is created. To view the requirement history, right click on the requirement to view the Requirement History

dialog. This dialog contains the details of each version of the requirement stored in the database.

### 15.7 Searching requirement text

It is possible to search for a requirement with a particular text string, by selecting the Requirement Management/Find menu option, to open the Find Requirement dialog. This Find dialog is very similar to the Find dialog found in many WYSIWYG applications. This search function only works for requirements which are currently loaded in the Requirements editor.

### 15.8 Requirements traceability

Normally requirements traceability is synonymous with adding a goal refinement association but, requirements may also contribute to vulnerabilities (as well as tasks), or be supported by assets or misuse cases. Consequently, requirements can be manually traced to these artifacts in the same manner as tasks.

### 15.9 Requirement association

A requirement associated to an environment can be associated with an asset, or a requirement associated with an asset can be associated with another asset. To re-associate a requirement, right click on the requirement, select Asset re-association, and select the asset to re-associate the requirement with.

## 16 Security Patterns

### 16.1 Overviews

Security Patterns are solution structures, which prescribe a solution to a security problem arising in a context. Many components and connectors in secure system architectures are instances of security patterns but, in many cases, the reasoning for a given pattern's inclusion is not always clear. The requirements needed to realise these patterns are also often omitted, making the job of reasoning about the consequences of situating the pattern difficult. Moreover, security patterns may be described in a context, but not all collaborating assets in a security pattern may be evident in all possible contexts of a system's use. The following sections describe how CAIRIS treats security patterns and deals with these weaknesses.

Security Patterns in CAIRIS consist of the following elements:

- A description of the context a pattern is relevant for.
- A problem statement motivating the need for the pattern.
- A solution statement describing the intrinsics of the pattern.
- The pattern structure, modelled as associations between collaborating asset classes.
- A set of requirements, which need to be fulfilled in order to realise the pattern.

Before a security pattern can be defined in CAIRIS, template assets – which represent the collaborating asset classes – need to be first defined.

Before a security pattern can be situated in CAIRIS environments, the environments themselves need to be first created.

## 16.2 Create a template asset

Template assets can be best described as context-free assets. When they are created, template assets do not form part of analysis unless they are implicitly introduced. This ‘implicit introduction’ occurs when a security pattern is situated (see section *situatesecuritypattern* (section 16.4)).

The Template Patterns dialog can be opened by selecting the Options/Template Assets menu option.

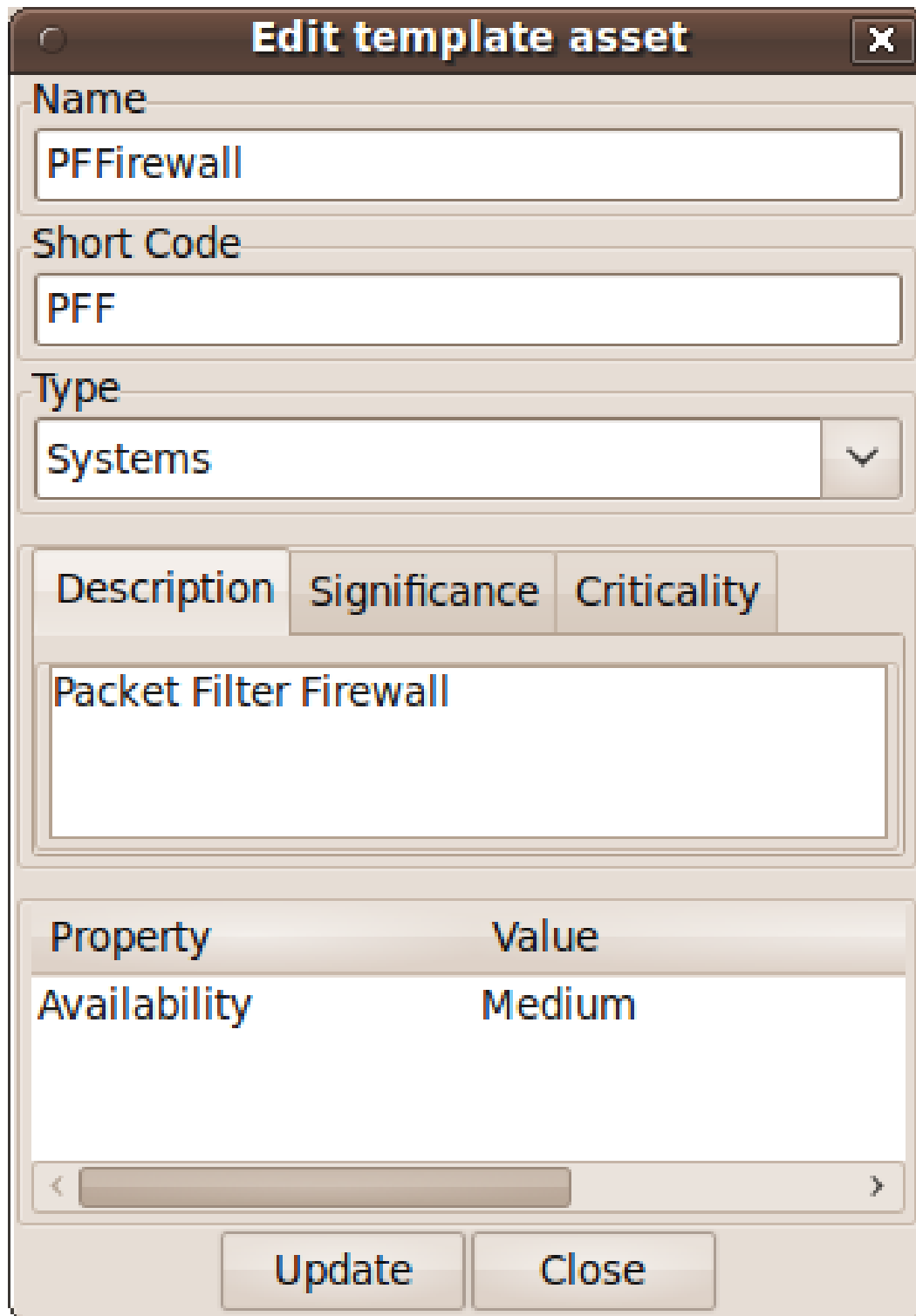
The process for creating, updating, and deleting a template asset is almost identical to the processes for normal assets. The only difference is the lack of environment-specific properties. Security properties are only defined once for the asset.

To situate an asset in an environment, right click on the template asset name in the Template Assets dialog box, select the Situate option, and specify the environments to situate the template asset in. After a template asset is situated within an environment, these properties should be revised in the assets generated on the basis of these. This is because the values associated with the template asset properties may not be inline with assumptions held about Low, Medium, and High assets in the specification being developed.

## 16.3 Create a security pattern

- Select the Options/Security Patterns menu option to open the Security Patterns dialog box, and click on the Add button to open the Security Pattern dialog box.
- Enter the security pattern name, and, in the Context page, type in a description the security pattern is relevant for.
- Click on the Problem page, and type in a problem description motivating the security pattern.
- Click on the solutionm page, and type in the intrinsics of how the security pattern solves the pre-defined problem.
- Click on the Structure page, and right-click on the association list control to add associations between template assets; these associations form the collaborative structure for the pattern. The procedure for entering associations is based on that used for associating assets.
- Click on the Requirements page, and right-click on the requirements list control to add requirements needing to be satisfied to realise the pattern. The cells in the Add Pattern Requirement dialog are a sub-set of those found in the CAIRIS requirements editor.
- Click on the Create button to add the new security pattern.





The dialog box is titled "Edit template asset" and contains several input fields and a table. The "Name" field contains "PFFirewall", the "Short Code" field contains "PFF", and the "Type" dropdown menu is set to "Systems". Below these fields are three tabs: "Description", "Significance", and "Criticality". The "Description" tab is active, showing a text area with "Packet Filter Firewall". At the bottom is a table with two columns: "Property" and "Value". The table has one row with "Availability" and "Medium". There are "Update" and "Close" buttons at the bottom right.

Property	Value
Availability	Medium

Figure 27: Template Pattern Dialog

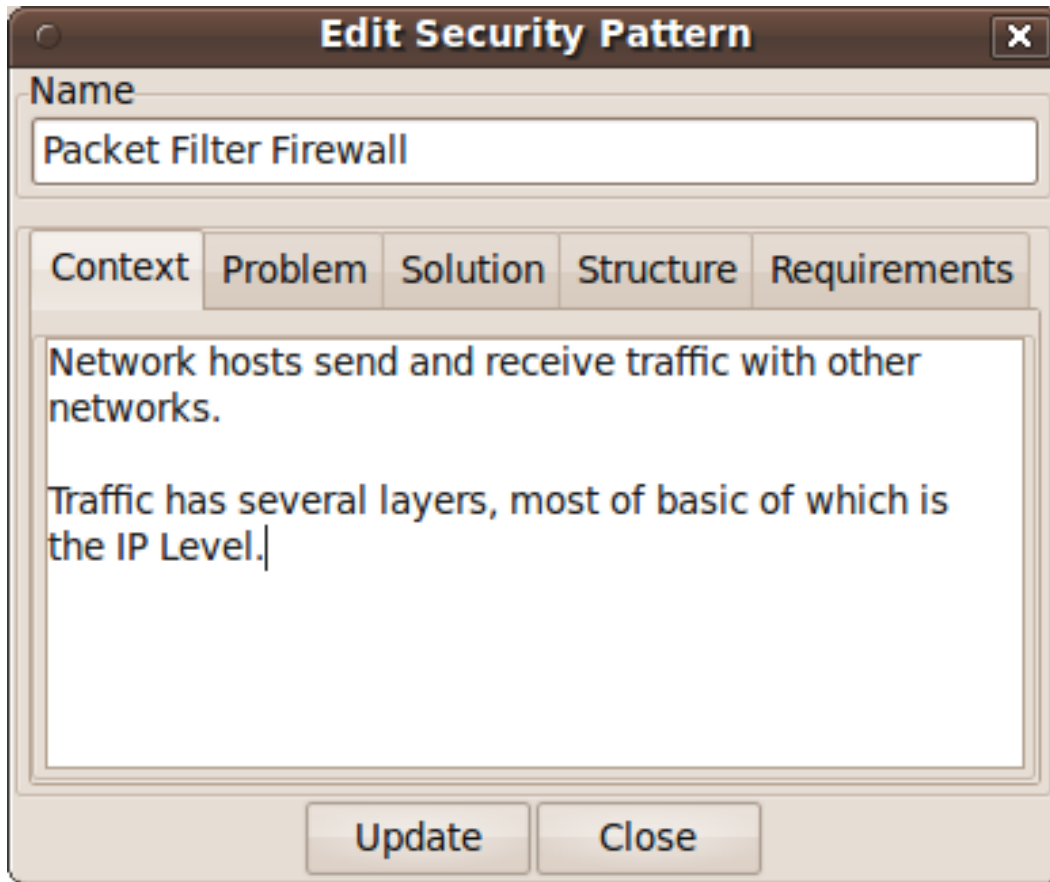
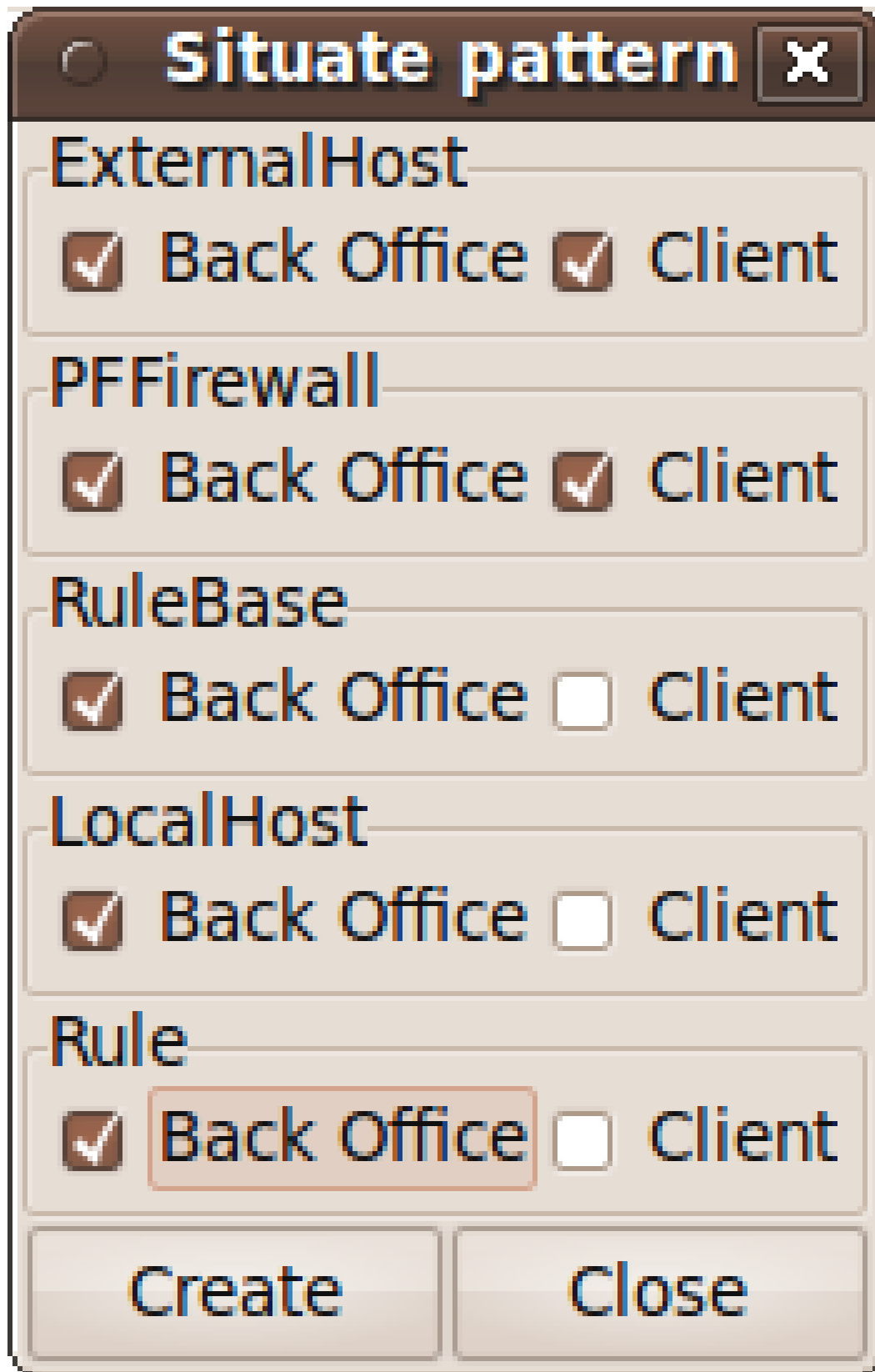


Figure 28: Security Pattern Dialog

- Existing security patterns can be modified by double clicking on the security pattern in the Security Patterns dialog box, making the necessary changes, and clicking on the Update button.
- To delete a security pattern, select the pattern to delete in the Security Patterns dialog box, and select the Delete button.

#### 16.4 Situate a security pattern

- To introduce a security pattern into the working project, open the Security Patterns dialog box, right-click on the pattern, and select the Situate Pattern option from the speed menu. This opens the Situate Pattern Dialog box, illustrated in figure fig:SituatePatternDialog (Figure 29).
- For each collaborating asset, click on the check boxes that you wish to situate each asset in. It may be that not all assets in the pattern are relevant for all contexts of use. Therefore, all the pattern structure is retained in the project, the pattern structure



The image shows a graphical user interface window titled "Situating pattern" with a close button (X) in the top right corner. The window contains five sections, each with a title and two checkboxes labeled "Back Office" and "Client".

Section	Back Office	Client
ExternalHost	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
PFFirewall	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
RuleBase	<input checked="" type="checkbox"/>	<input type="checkbox"/>
LocalHost	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Rule	<input checked="" type="checkbox"/>	<input type="checkbox"/>

At the bottom of the window are two buttons: "Create" and "Close".

Figure 29: Situate Pattern Dialog

displayed in each environment is based only on the assets situated. For example, for the Packet Filter Pattern, an end-user context of use may only be concerned with the client workstation asset and the firewall. A system administrator may be concerned about most of the pattern structure, but may be less concerned about interactions with external hosts.

- Click on the Create button to situate the pattern.

Template assets will be instantiated as assets, and situate in the stipulated assets. Requirements associated with the pattern, will be introduced and associated with the stipulated assets in the pattern definition. These assets will be ordered based on the order of definition in the pattern structure.

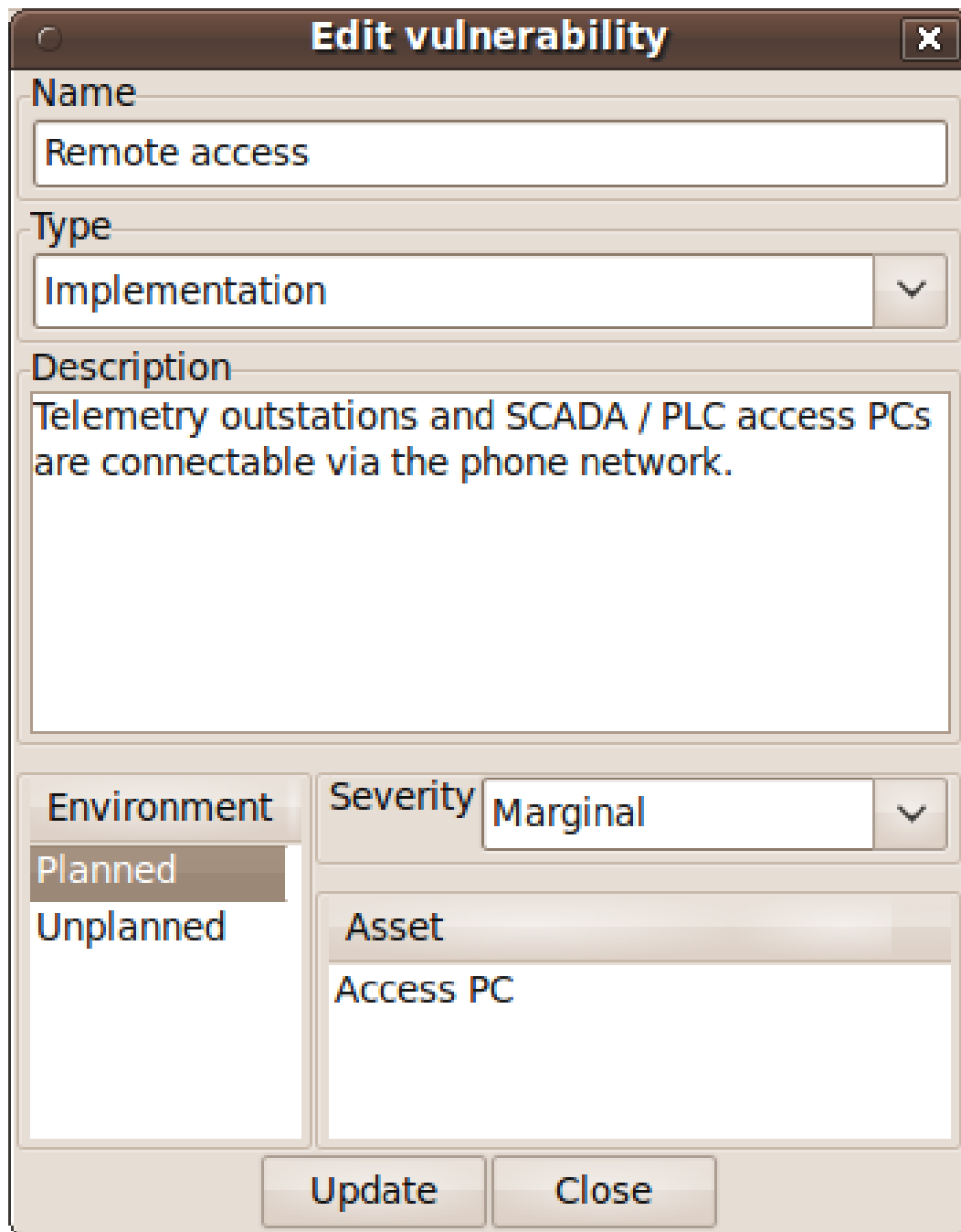
## 17 Vulnerabilities

### 17.1 Overview

Vulnerabilities are weaknesses of a system, which are liable to exploitation.

### 17.2 Create a vulnerability

- Click on the Vulnerability toolbar button to open the Vulnerabilities dialog box.
- Click on the Add button to open the Create Vulnerability dialog box.
- Enter the vulnerability name and description, and select the vulnerability type from the combo box.
- Right click on the environment window to bring up the environment speed menu. Select the add option and, from the Add environment window, select an environment to situate the vulnerability in. This will add the new environment to the environment list.
- After ensuring the environment is selected in the environment window, select the vulnerability's severity for this environment, and add exposed assets by right clicking on the asset box and selecting one or more assets from the selected environment.
- Click on the Create button to add the new vulnerability.
- Existing vulnerabilities can be modified by double clicking on the vulnerability in the Vulnerabilities dialog box, making the necessary changes, and clicking on the Update button.
- To delete a vulnerability, select the vulnerability to delete in the Vulnerabilities dialog box, and select the Delete button. If any artifacts are dependent on this vulnerability then a dialog box stating these dependencies are displayed. The user has the option of selecting Yes to remove the vulnerability dependencies and the vulnerability itself, or No to cancel the deletion.



The image shows a software dialog box titled "Edit vulnerability". It contains several input fields and a list. The "Name" field is labeled "Name" and contains the text "Remote access". The "Type" field is labeled "Type" and contains a dropdown menu with "Implementation" selected. The "Description" field is labeled "Description" and contains the text "Telemetry outstations and SCADA / PLC access PCs are connectable via the phone network." Below these fields, there is a section with two columns. The left column is labeled "Environment" and contains a list with "Planned" and "Unplanned" items. The right column is labeled "Severity" and contains a dropdown menu with "Marginal" selected. Below the "Severity" dropdown, there is a section labeled "Asset" which contains a text field with the text "Access PC". At the bottom of the dialog, there are two buttons: "Update" and "Close".

**Edit vulnerability**

Name  
Remote access

Type  
Implementation

Description  
Telemetry outstations and SCADA / PLC access PCs are connectable via the phone network.

Environment  
Planned  
Unplanned

Severity  
Marginal

Asset  
Access PC

Update Close

Figure 30: Vulnerability Dialog

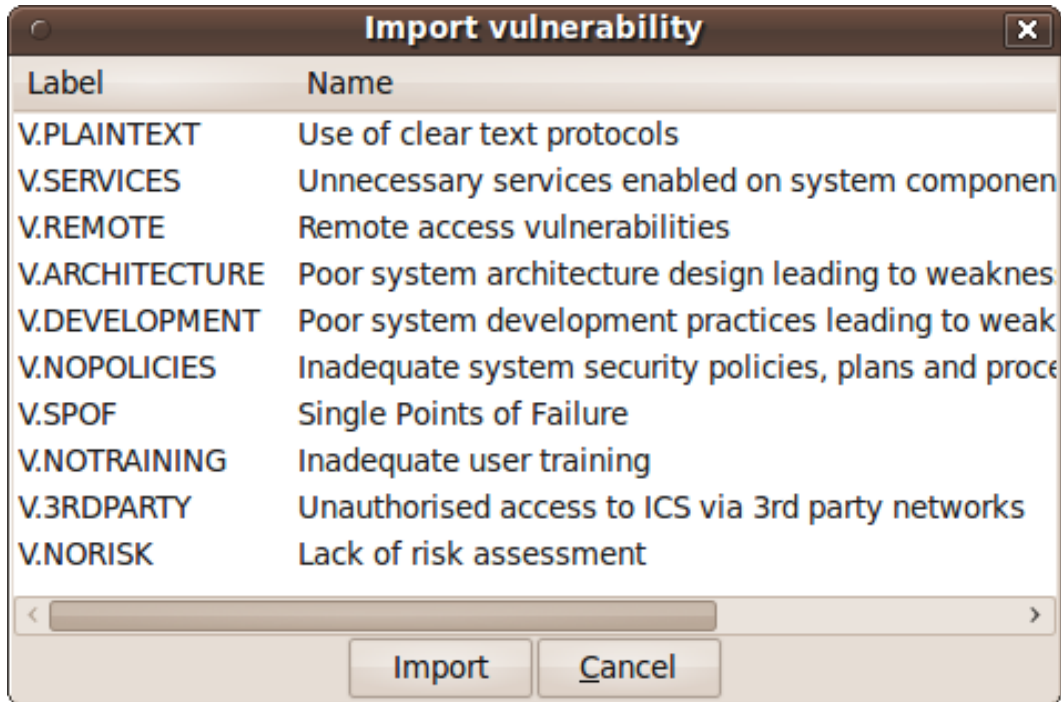


Figure 31: Import Vulnerability

### 17.3 Importing a vulnerability

The CAIRIS database is pre-loaded with a database of template vulnerabilities based on the Common Criteria. To import one of these, select Import from the Vulnerabilities dialog to open the Import Vulnerability dialog (figure [fig:ImportVulnerability]). When a vulnerability is selected, the Vulnerability dialog is opened, and pre-populated with information from the template, as indicated in figure fig:ImportedVulnerabilityDialog (Figure 32).

## 18 Attackers

### 18.1 Overview

Attackers launch attacks in the form of threats. Attackers are similar to personas in that fulfil one or more roles, and can be personalised with additional information.

Certain capabilities and motivations may be associated with attackers. CAIRIS is pre-loaded with a selection of these, but these can be modified, or new capabilities and motivations created by selecting the Options/Capabilities or Options/Motivations menu options.

### 18.2 Adding, updating, and deleting an attacker

- Click on the Attacker toolbar button to open the Attackers dialog box, and click on the Add button to open the Attacker dialog box.

**Import vulnerability**

Name  
V.PLAINTEXT

Type  
Design

Description  
Use of clear text protocols  
The use of clear text protocols and the transmission of business and control data unencrypted over insecure communication channels (e.g. FTP, TELNET)

Environment  
Severity

Asset

Update Close

Figure 32: Imported Vulnerability

- Enter the attacker name, and a description for the attacker.
- If you have decided to personalise the attacker with a picture, this can be added by right clicking on photo box next to the attacker description, to bring up the Load Image option from the speed menu, and selecting Load Image. Please note that the image itself is NOT imported into the database, only the file path to the picture.
- Right click on the environment window to bring up the environment speed menu. Select the add option and, from the Add environment window, select an environment to situate the attacker in. This will add the new environment to the environment list.
- After ensuring the environment is selected in the environment window, right-click on the Roles list, and select Add from the speed menu to associate one or more roles to the attacker.
- Right-click on the Motive and Capability boxes and select Add to add one or more motive and capability values. For the capability, a value of Low, Medium, or High also needs to be selected.


Edit attacker

Name

Victor

Description

Victor is contractor and expert in the SCADA systems, having helped develop these 15 years ago. As these systems are beginning to get phased out, Victor thinks it might be time to retrain in some of the newer SCADA technologies in use.  
  
Victor recently applied for a job at the organisation who



Environment

Planned

Unplanned

Role

Engineer

Motive

Revenge

Capability	Value
Resources/Personnel and Time	Medium
Knowledge/Education and Training	High

<

>

Update

Close

Figure 33: Attacker Dialog



- Click on the Create button to add the new attacker.
- Existing attackers can be modified by double clicking on the attacker in the Attackers dialog box, making the necessary changes, and clicking on the Update button.
- To delete an attacker, select the attacker to delete in the Attackers dialog box, and select the Delete button. If any artifacts are dependent on this attacker then a dialog box stating these dependencies are displayed. The user has the option of selecting Yes to remove the attacker dependencies and the attacker itself, or No to cancel the deletion.

## 19 Threats

### 19.1 Overview

Threats are synonymous with attacks, and can therefore only be defined if an associated attacker has also been defined. Like vulnerabilities, threats are associated with one or more assets. However, threats may also target certain security properties as well, in line with security values that an attacker wishes to exploit.

A threat is also of a certain type. CAIRIS is pre-loaded with a selection of these, but these can be modified, or new threat types created by selecting the Options/Threat Types menu option.

### 19.2 Adding, updating, and deleting a threat

- Click on the Threat toolbar button to open the Threats dialog box, and click on the Add button to open the Threat dialog box.
- Enter the threat name, the method taken by an attacker to release the threat, and select the threat type.
- Right click on the environment window to bring up the environment speed menu. Select the add option and, from the Add environment window, select an environment to situate the threat in. This will add the new environment to the environment list.
- After ensuring the environment is selected in the environment window, select the threat's likelihood for this environment
- Associate attackers with this threat by right clicking on the attacker box, selecting Add from the speed menu, and selecting one or more attackers associated with the environment.
- Add threatened assets by right clicking on the asset box, selecting Add from the speed menu, and selecting one or more assets from the selected environment.
- Add the security properties to this threat by right clicking on the properties list, and selecting Add from the speed menu to open the Add Security Properties window. From this window, a security property and its value can be added.
- Click on the Create button to add the new threat.

**Edit threat**

Name  
Logic bomb

Type  
Insider/Sabotage

Method  
A logic bomb incorporated into PLC software to cause a plant failure upon a set of conditions.

Environment  
Planned

Likelihood  
Improbable

Attacker  
Bob  
Victor

Asset  
PLC Software

Property	Value
Accountability	High

Update Close

Figure 34: Threat Dialog

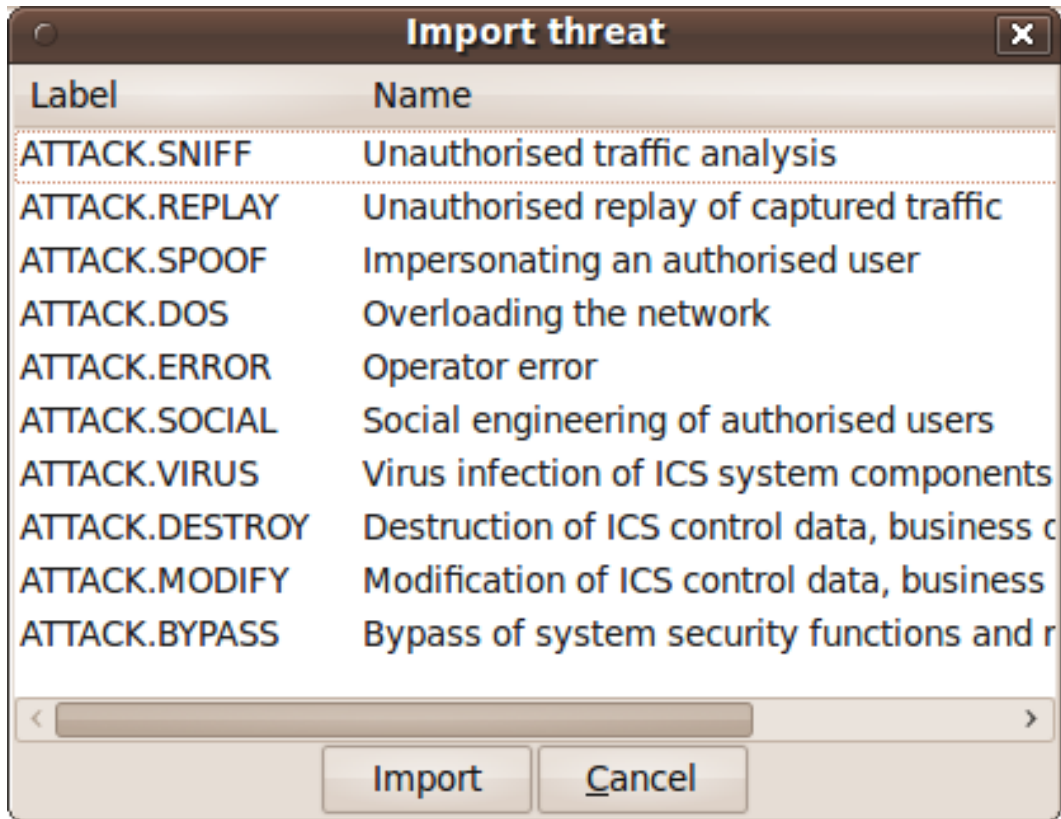


Figure 35: Import Threat

- Existing threats can be modified by double clicking on the threat in the Threats dialog box, making the necessary changes, and clicking on the Update button.
- To delete a threat, select the threat to delete in the Threats dialog box, and select the Delete button. If any artifacts are dependent on this attacker then a dialog box stating these dependencies are displayed. The user has the option of selecting Yes to remove the threat dependencies and the threat itself, or No to cancel the deletion.

### 19.3 Importing threats

The CAIRIS database is pre-loaded with a database of template threats based on the Common Criteria. To import one of these, select Import from the Threats dialog to open the Import Threat dialog (figure [fig:ImportThreat]). When a threat is selected, the Threat

dialog is opened, and pre-populated with information from the template.


## 20 Risks

### 20.1 Overview

Risks are defined as the detriment arising from an attacker launching an attack, in the form of a threat, exploiting a system weakness, in the form of a vulnerability. Associated with each risk is a Misuse Case. A Misuse Case describes how the attacker (or attackers) behind the risk's threat exploits the risk's vulnerability to realise the risk.

The current status of Risk Analysis can be quickly ascertained by viewing the Risk Analysis model. This displays the current risks, the artifacts contributing to the risk, and the artifacts which potentially mitigate it.

### 20.2 Adding, updating, and deleting a risk

- Click on the Risk toolbar button to open the Risks dialog box, and click on the Add button to open the Risk dialog box.
- Enter a risk name and select a threat and vulnerability from the respective combo boxes. A risk is valid only if the threat and vulnerability exist within the same environment (or environments).
- Highlighting the environment name in the environment box displays a qualitative risk rating, and the mitigated and un-mitigated risk score associated with each risk response. To see how this score is calculated, click on the Show Details button.
- Before a risk can be created, an associated Misuse Case needs to be defined. To do this, click on the Create Misuse Case button to open the Misuse Case Dialog (figure ) (Figure 37)).
- Most of the fields in the Misuse Case dialog have already been completed based on the risk analysis carried out up to this point. Click on the Narrative tab and enter a scenario which describes how the attacker realises the associated risk, i.e. carries out the threat by exploiting the vulnerability. The scenario written should be written in line with the attributes and values displayed in the Summary tab.
- Click on the Create button to create the Misuse Case and close the Misuse Case Dialog. Following this, click Create add the new risk.
- Existing risks can be modified by double clicking on the risk in the Risks dialog box, making the necessary changes, and clicking on the Update button.
- To delete a risk, select the risk to delete in the Risks dialog box, and select the Delete button. If any artifacts are dependent on this risk then a dialog box stating these dependencies are displayed. The user has the option of selecting Yes to remove the risk dependencies and the risk itself, or No to cancel the deletion.

**Edit risk**

Name  
Plant logic bomb via borrowed credentials

Threat  
Logic bomb

Vulnerability  
Credentials sharing

Environments  
Planned

Rating  
Tolerable

Response	Unmit. Score	Mit. Score
Detect Plant logic bomb via borro...	9	1

Show Details

Update Edit Misuse Case Close

Figure 36: Risk Dialog

### 20.3 Risk Analysis model

Risk Analysis models can be viewed by clicking on the Risk Analysis Model toolbar button, and selecting the environment to view the environment for.

By changing the environment name in the environment combo box, the risk analysis model for a different environment can be viewed. The layout of the model can also be replaced by selecting a layout option in the Layout combo box at the foot of the model viewer window.

By clicking on a model element, information about that artifact can be viewed.

The risk analysis model can also be filtered by artifact type and artifact type. Filtering by type displays only the artifacts of the filtered type, and its directly associated assets. Filtering by artifact name displays only the filtered artifact, and its directly associated

**Edit Misuse Case**

Name  
Exploit Plant logic bomb via borrowed credentials

Risk  
Plant logic bomb via borrowed credentials

Environment  
Planned

Summary Narrative

Objective  
Exploit vulnerabilities in Windows login Credentials to threaten PLC Software.

Attacker  
Bob  
Victor

Asset  
PLC Software  
Windows login Credentials

Threat  
Logic bomb

Likelihood  
Improbable

Vulnerability  
Credentials sharing

Severity  
Critical

Risk Rating  
Tolerable

Update Close

Figure 37: Misuse Case Dialog

artifacts.

## 21 Risk Responses

A risk can be treated in several ways.

By choosing to *Accept* a risk, we indicate that we are prepared to accept the consequences of the risk being realised. Accepting the risk comes with a cost, and responsibility for accepting a risk must fall on one or more roles.

By choosing to *Transfer* a risk, we acknowledge that dealing with a risk is out of scope for this project. It may still, however, have a cost associated with it and, by accepting the risk, the risk must become the responsibility of one or more roles.

By choosing to *Mitigate* a risk, we may either Prevent, Deter, Detect, or React to a risk. For detective responses, the response must detect the risk before, during, or after the risk's realisation. For reactive responses, the response must be associated with an countermeasure asset derived from a detective response.

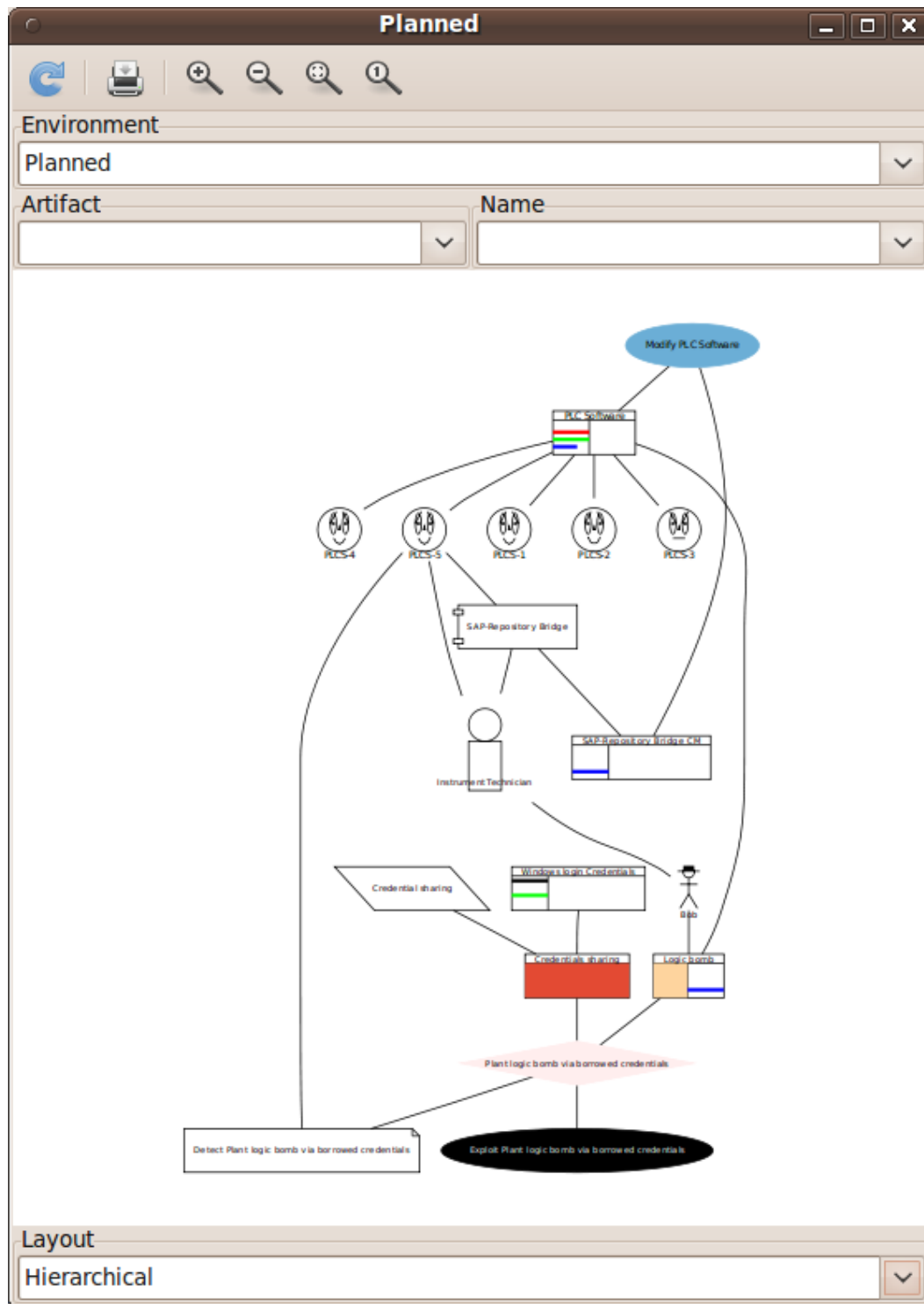


Figure 38: Risk Analysis Model

**Edit response**

Name  
Detect Plant logic bomb via borrowed credentials

Risk  
Plant logic bomb via borrowed credentials

Environment  
Planned

Type  
Detect

Detection Point  
After

Detection Mechanism

Update Close

Figure 39: Response Dialog

### 21.1 Adding, updating, and deleting a response

- Click on the Response toolbar button to open the Responses dialog box, and click on the Add button. Select the response to take from the available options presented.
- Select the risk to associate this response with.
- Right click on the environment window to bring up the environment speed menu. Select the add option and, from the Add environment window, select an environment



to situate the response in. This will add the new environment to the environment list.

- After ensuring the environment is selected in the environment window, select the response type.
- When the risk name and response type is selected, the response name is automatically generated.
- If an accept or transfer response was selected, a cost and rationale needs to be entered. For transfer responses, one or more roles also need to be associated with the response.
- If a Detect response is selected, select the Detection Point (Before, Medium, or After).
- If a React response is selected, right click on Detection Mechanism box, select Add from the speed menu, and select a detection mechanism asset.
- Click on the Create button to add the new response.
- Existing responses can be modified by double clicking on the response in the Responses dialog box, making the necessary changes, and clicking on the Update button.
- To delete a response, select the response to delete in the Responses dialog box, and select the Delete button. If any artifacts are dependent on this response then a dialog box stating these dependencies are displayed. The user has the option of selecting Yes to remove the response dependencies and the response itself, or No to cancel the deletion.

## 21.2 Generating goals

A goal can be generated from a response by right clicking on the response name in the Responses dialog box, and selecting Generate Goal from the speed menu. This causes a goal to be generated in each of the environments the response is situated in. The goal name corresponds to the name of the response.

## 22 Countermeasure Design

After a response goal has been generated, goal modelling continues until one or more countermeasure requirements have been defined and associated with their parent goals. Following this, a countermeasure can be defined. Defining a countermeasure also has the effect of satisfying a response goal and resolving any obstacles associated with the underlying risk's threat or vulnerability.

Countermeasures target a risk's threat, vulnerability, or both. Countermeasures also have a level of effectiveness. This effectiveness level determines how much the countermeasure reduces the likelihood of the associated threat, or severity of the associated vulnerability.

Countermeasures are associated with roles, who may be responsible for developing, maintaining or using the countermeasure. Consequently, countermeasures are also associated with tasks and, when defining a countermeasure, it is also necessary to indicate how much the countermeasure helps or hinders the properties of associated tasks.

**Edit countermeasure**

Name: Peer review plugin

Type: Software

Description: The software repository shall incorporate a plugin which randomly assigns PLC software modifications to other instrument technicians or engineers for review.

Environment: Planned

Cost: High

**Security** Usability

Requirement	Target	Effectiveness
PLCS-9	Credentials sharing	High

Property	Value
Accountability	High

Update Close

Figure 40: Countermeasure Dialog: Security Page

### 22.1 Adding, updating, and deleting a countermeasure

- Click on the Countermeasure toolbar button to open the Countermeasures dialog box, and click on the Add button to open the Countermeasure dialog box.
- Enter the countermeasure name and description, and select the countermeasure type. A countermeasure may be one of the following type: Information, Systems, Software, Hardware, or People.
- Right click on the environment window to bring up the environment speed menu. Select the add option and, from the Add environment window, select an environment to situate the countermeasure in. This will add the new environment to the environment list.
- After ensuring the environment is selected in the environment window, select the countermeasure cost

**Edit countermeasure**

Name: Peer review plugin

Type: Software

Description: The software repository shall incorporate a plugin which randomly assigns PLC software modifications to other instrument technicians or engineers for review.

Environment: Planned

Cost: High

Security Usability

Role: Engineer, Instrument Technician

Task	Persona	Duration	Frequency	Demands	Goals
Modify Telemetry Software...	Barry	None	None	None	None
Modify PLC Software	Barry	None	None	None	None
Modify SCADA HMI software	Barry	None	None	None	None

Update Close

Figure 41: Countermeasure Dialog: Usability Page

- Click on the Security tab to display the security page (figure fig:CountermeasureDialogSecurity (Figure 40)). Right click in the Requirements box, and select add from the speed menu to add the requirement (or requirements) this countermeasure refines. Following this, right click on the Target list and select add to select the countermeasure's target/s, together with the countermeasure's effectiveness. Finally, add the security properties fostered by this countermeasure via the security properties box at the bottom of the page.
- Click on the Usability tab to display the usability page (figure fig:CountermeasureDialogUsability (Figure 41)). Right click on the Roles box, and select add from the speed menu to add the roles associated with this countermeasure. Any tasks associated with these roles are automatically populated in the Task box at the bottom of the page, together with the person/s carrying out the task. If the countermeasure helps or hinders a task, double click on the task and modify the task's attributes accordingly.
- Click on the Create button to add the new countermeasure.
- Existing countermeasures can be modified by double clicking on the countermeasure in the Countermeasures dialog box, making the necessary changes, and clicking on the Update button.

- To delete a countermeasure, select the countermeasure to delete in the Countermeasures dialog box, and select the Delete button. If any artifacts are dependent on this countermeasure then a dialog box stating these dependencies are displayed. The user has the option of selecting Yes to remove the countermeasure dependencies and the countermeasure itself, or No to cancel the deletion.

## 22.2 Generating countermeasure assets and security patterns

By right clicking on a countermeasure in the Countermeasures window, an associated asset can be generated. If defined, this will retain the same security properties associated with the countermeasure. The asset will be situated in whatever environments the countermeasure was situated in. In the asset model, a << safeguard >> association is added between the countermeasure asset and any assets threatened or exposed by the risk the countermeasure helps mitigate.

Assets can be generated directly based on the countermeasure properties, or on the basis of a pre-existing template asset. It is also possible to situate security patterns based on a countermeasure, rather than an asset. To do this, select Situate Pattern from the speed menu, select the security pattern, followed by the countermeasure environments to situate the pattern assets in.

Security Patterns can be imported into the tool by using the Import/Import Security Patterns option, and selecting the XML based patterns catalogue to import. An example catalogue file, *schumacher.xml*, which incorporates a number of patterns from the Security Patterns text book by Schumacher et al is included in the *iris/sql* directory.

## 22.3 Associating countermeasures with pre-existing patterns

By right clicking on a countermeasure in the Countermeasures window, you can also associate a countermeasure with a pre-existing security pattern by selecting the 'Associate with situated Countermeasure Pattern' option. However, a list of possible security patterns to choose from will only be displayed if the components of the security pattern are present in ALL of the environments the countermeasure is situated for.

## 22.4 Weaking the effectiveness of countermeasures

Countermeasures mitigate risks by targetting its risk elements, i.e. its threats or vulnerabilities. However, when one or more assets are generated from these countermeasures, several factors may weaken the effect of the countermeasure.

First, situating assets may cause you to look at the environments where the assets are situated in a different light. Changing properties of assets, or existing threats or vulnerabilities could increase the potency of the risk, thereby weakening the effect of the countermeasure.

Existing threats or vulnerabilities can also explicitly weaken countermeasures. If a countermeasure asset is associated with a threat or vulnerability then, when either artifact is created or modified, CAIRIS allows users to override the effectiveness of the related countermeasure. The detail associated with the risk scores in the Risk Dialog box will indicate cases where countermeasures have been weakened by threats and/or vulnerabilities.

### 22.5 Mitigating weakening effects

If a countermeasure is weakened, the weakness is removed by generating a new countermeasure which targets the weakening threat or vulnerability. If this is carried out, the detail associated with the risk score in the Risk Dialog box will indicate cases where, although the effectiveness score for the countermeasure holds, this is by virtue of a countermeasure targeting the weakening threat or vulnerability.

Countermeasures cannot, however, be simply defined on the fly. They arise as the result of rational risk analysis, so risks need to be defined based on the weakening threats or vulnerabilities.

## 23 Generating Documentation

The current contents of the CAIRIS database can be generated as a requirements specification by selecting the Generate Documentation toolbar button. After the sections to be included are selected in the Generate Documentation dialog box (figure `fig:GenerateDocumentationDialog` (Figure 42)), the target directory is prompted, following which the specification is generated as HTML, RTF, or PDF, based on the output options selected.

