
Grant Agreement: 287829

Comprehensive Modelling for Advanced Systems of Systems

COMPASS

# Theorem Proving Support - User Manual

Technical Note Number: D33.2a

Version: 1.0

Date: September 2013

Public Document

http://www.compass-research.eu

## Contributors:

Simon Foster, UY
Richard Payne, NCL

## Editors:

Simon Foster, UY
Richard Payne, NCL

## Reviewers:

Juliano Iyoda, UFPE
Jan Peleska, UB
Luís D. Couto, AU

# Document History

| Ver | Date | Author | Description |
|---|---|---|---|
| 0.01 | 18-06-2013 | Richard Payne | Initial document version |
| 0.02 | 02-07-2013 | Richard Payne | Added details on obtaining, installing and using Isabelle |
| 0.03 | 16-07-2013 | Richard Payne | Initial draft of document for first milestone |
| 0.04 | 29-08-2013 | Richard Payne | Changes throughout – to support ongoing work and to include details on proving in Isabelle perspective |
| 0.05 | 04-09-2013 | Richard Payne | Final changes to reflect tool updates |
| 0.06 | 18-09-2013 | Richard Payne/Simon Foster | LDC review comments addressed |
| 0.07 | 23-09-2013 | Richard Payne | JI review comments addressed |
| 1.0 | 26-09-2013 | Richard Payne | Final revision for EC |

# Summary

Work Package 33 delivers a collection of static analysis tool support for reasoning in CML. This deliverable forms the documentation for Task 3.3.2 – theorem proving. Deliverable D33.2 forms two parts: executable code and documentation.

The executable code is provided as described in Section 2, and the documentation is provided in two documents. This document, D33.2a, is the first part; the user manual, which provides details on obtaining and installing the theorem proving support for CML, and also how to use this support within the CML platform inside Eclipse. The second part of the D33.2 documentation, the technical details of the theorem proving support, is provided in document D33.2b.

# Contents

# 1 Introduction

This document is a user manual for the theorem proving support provided by the COMPASS tool, an open source tool supporting systematic engineering of System of Systems using the COMPASS Modelling Language (CML). This document is targeted at users with limited experience working with Eclipse-based tools. Directions are given as to where to obtain the software.

This user manual does not provide details regarding the underlying CML formalism. Thus if you are not familiar with this, we suggest the tutorial for CML before proceeding with this user manual [WCF+12, BGW12]. However, users broadly familiar with CML may find the Tool Grammar reference (COMPASS Deliverable D31.2c [Col13]) useful to ensure that the they are using the exact syntax accepted by the tool.

This version of the document supports version 0.1.4 and later of the COMPASS tool suite. The intent is to introduce readers to how use the theorem proving support plugin available in this version of the tool. The main tool is the COMPASS IDE, which integrates all of the available CML analysis functionality and provides editing abilities.

Section 2 describes how to obtain the software. Section 3 describes how to install the software in the COMPASS tool, Section 4 explains how to use the COMPASS Eclipse perspective and Section 5 describes how to prove theorems in the COMPASS tool. Conclusions are drawn in Section 6.

It should be noted that it is beyond the scope of this document to provide detailed descriptions of how to prove theorems in the Isabelle tool, or to provide a tutorial on it's use. We therefore recommend that interested parties should read this deliverable in conjunction with tutorials on Isabelle and proving in the Isabelle tool, available on the Isabelle website[1].

[1] http://isabelle.in.tum.de/documentation.html

# 2 Obtaining the Software

This manual assumes the user has the version 0.2.0 or later of the COMPASS tools pre-installed. The COMPASS tool set may be obtained from:

`http://sourceforge.net/projects/compassresearch/files/Releases/`

For instructions on installation, see the COMPASS user manual [CMLC13]. To use the theorem proving functionality of the tools, the Isabelle theorem prover and UTP/CML theory files must first be obtained. This is described in this section.

## 2.1 Isabelle

Isabelle is a free application, distributed under the BSD license. It is available for Linux, Windows and Mac OS X. The tool is available at:

`http://isabelle.in.tum.de`

Instructions for installation for each platform are provided in the following sections:

### 2.1.1 Mac OS X

Instructions for installation of Isabelle for Mac are as follows:

1. Download Isabelle for Mac, distributed as a dmg disk image.
2. Open the disk image and move the application into the */Applications* folder.
3. NOTE: Do not launch the tool at this point.

### 2.1.2 Windows

Instructions for installation of Isabelle for Windows are as follows:

1. Download Isabelle for Windows, distributed as an exe executable file.
2. Open the executable, which automatically installs the Isabelle tool.
3. NOTE: Do not launch the tool at this point.

### 2.1.3 Linux

Instructions for installation of Isabelle for Linux are as follows:

1. Download Isabelle for Linux, distributed as a tar bundled archive.
2. Unpack the archive into the suggested target directory.
3. NOTE: Do not launch the tool at this point.

## 2.2 UTP/CML Theories

To prove theorems and lemmas for CML models, Isabelle must have access to the UTP and CML Theories. Instructions for obtaining these theories are given below for different platforms:

### 2.2.1 Linux, Mac OS X

1. Download the latest version of the utp-isabelle-x archive from

   `https://sourceforge.net/projects/compassresearch/files/HOL-UTP-CML/`

   Linux/Mac can choose either .zip or .tar.bz2.

2. Extract the downloaded theory package and save the utp-isabelle directory to your machine, for example */home/me/Isabelle/utp-isabelle-0.x*.

As the CML and UTP theories are improved, new versions will be made available. As new versions are uploaded, follow the above steps to obtain and unpack the updates. See Section 3.4 for details of setting up updated theories.

### 2.2.2 Windows

1. Download the latest version of the utp-isabelle-x-windows.zip archive from

   `https://sourceforge.net/projects/compassresearch/files/HOL-UTP-CML/`

2. Extract the downloaded theory package.

3. Copy the *ROOTS* file from the extracted folder to the Isabelle2013 application folder (e.g. C:\Program Files\Isabelle2013\). Windows will warn you a ROOTS file already exists. This is ok – choose to replace the existing file.
4. Copy the *utp-isabelle* folder from the extracted folder to the src folder in the Isabelle2013 application folder (e.g. C:\Program Files\Isabelle2013\src\).

As the CML and UTP theories are improved, new versions will be made available. As new versions are uploaded, follow the above steps to obtain and unpack the updates. See Section 3.4 for details of setting up updated theories.

# 3 Instructions for installation of Isabelle/UTP

This section provides, the steps required to use Isabelle in the COMPASS tools. This setup procedure is only required on the first use of the theorem prover. However, if a new version of the COMPASS tools is installed, then the procedure must be repeated. Instructions for installation with the COMPASS tool are given for each supported platform below:

## 3.1 Mac OS X

1. Open the COMPASS Tool application.
2. From the menu bar, select *Run>Isabelle>Isabelle Configurations*.
3. Select *Isabelle Mac App* in the left hand pane, click the *'New Launch Configuration'* button (see Figure 1) and provide a name for the configuration: *Isabelle-CML*.

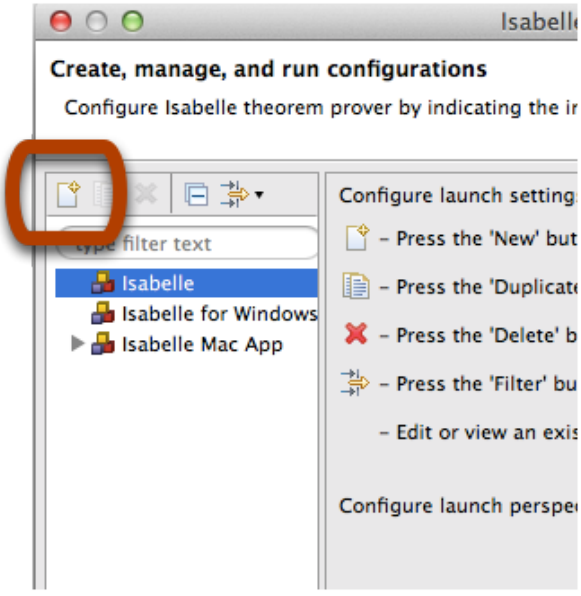


Figure 1: New Launch Configuration button

4. In the *Main* tab provide the location of the Isabelle application (for example */Applications/Isabelle2013.app*). Use the *'Browse File System...'* button to navigate to the correct location if required, see Figure 2. **NOTE: do not select a logic at this point**.

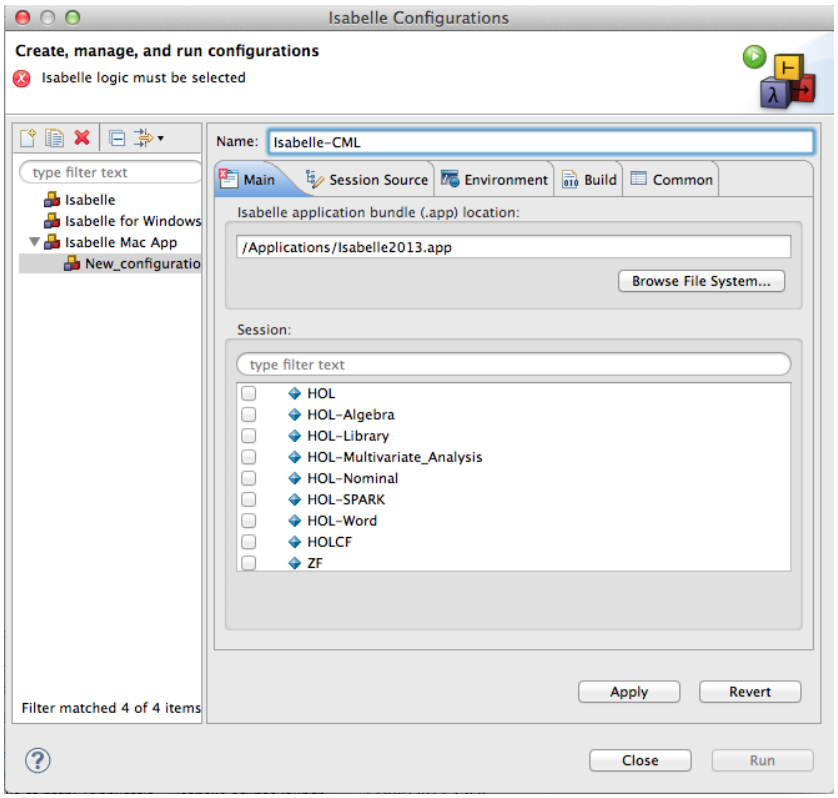


Figure 2: Isabelle configuration in COMPASS Tool – Mac

5. Select the *Session Source* tab, and click the *'Add external...'* button. Navigate to the location of the utp-isabelle folder extracted in Section 2.2, see Figure 3, and click *'Open'*.

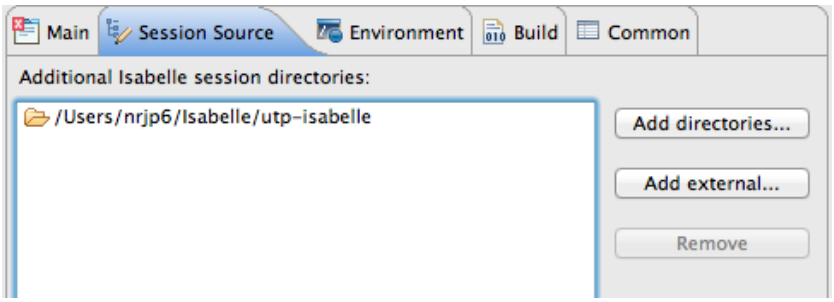


Figure 3: Isabelle configuration in COMPASS Tool – Session source

6. For licensing of the Z3 theorem prover used by the Isabelle tool[2], select the *Environment* tab, and click the *'New...'* button. In the *'Name:'* text box

[2]This part of the tool is available free for non-commercial use. For licens-

enter **Z3_NON_COMMERCIAL**, and in the *'Value:'* text box enter **yes**, see Figure 4, and click *'Ok'*. Ensure the *'Append environment to the native environment'* option is selected.

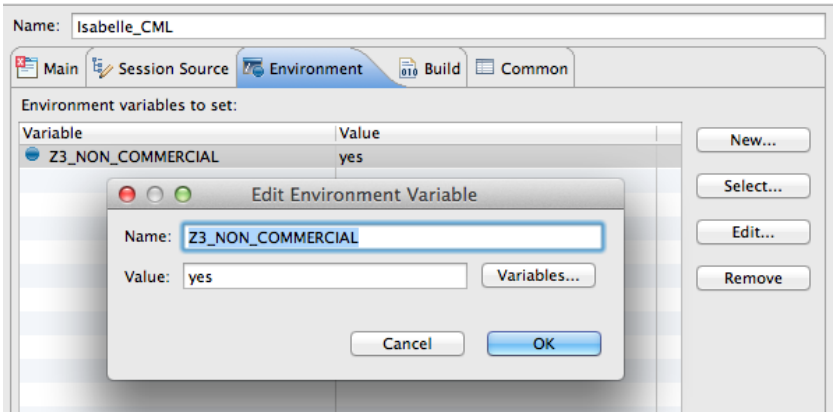


Figure 4: Isabelle configuration in COMPASS Tool – Environment

7. Select the *Build* tab, and select the *Build sessions to user home directory* button, see Figure 5.

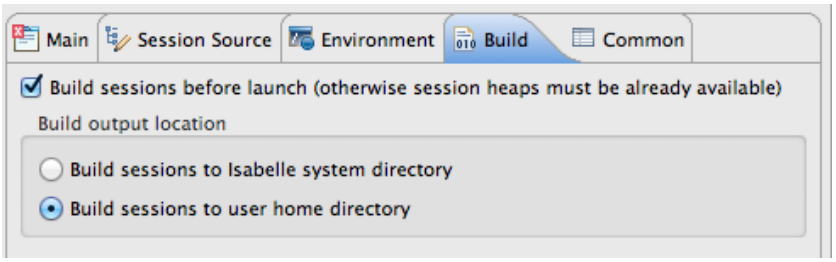


Figure 5: Isabelle configuration in COMPASS Tool – Build

8. Select the *Main* tab and in the *Session:* field, choose the *HOL-UTP-CML* logic (there is a filter text box which may help locate the correct logic, see Figure 6).

9. Click the *'Apply'* button to save the configuration, and click the *'Run'* button to start Isabelle. **NOTE:** the first time Isabelle is invoked, several minutes are needed to initialise and build the theories. Subsequent uses of Isabelle will not require this long wait. To monitor progress, click on the button on the bottom right of the tool, as highlighted in Figure 7.

ing information, see `http://www.microsoftstore.com/store/msuk/en_GB/pdp/Microsoft-Research-Z3-Theorem-Prover/productID.278142500`

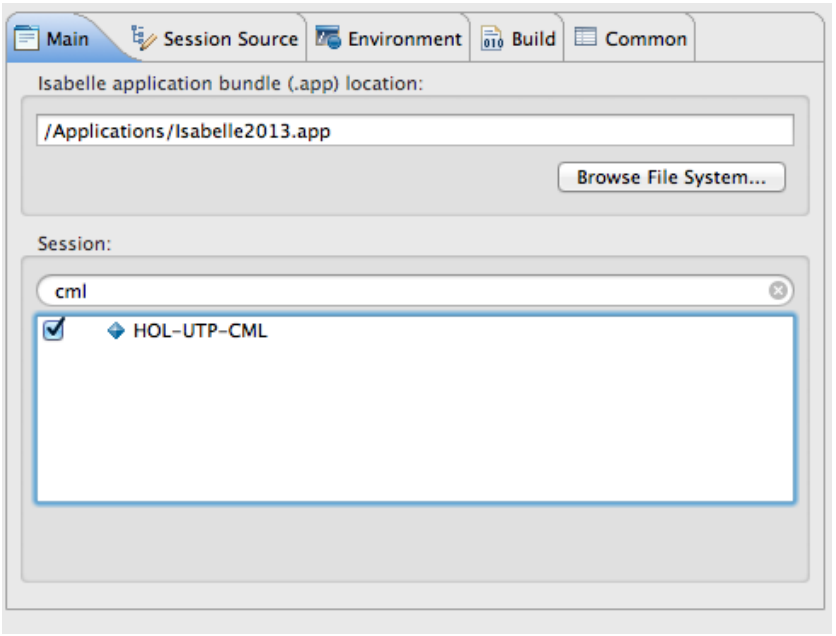


Figure 6: Isabelle configuration in COMPASS Tool – Selecting logic


Figure 7: Isabelle configuration in COMPASS Tool – initialisation progress.

## 3.2 Windows

1. Open the COMPASS Tool application.
2. Configure the COMPASS Tool to use Isabelle – From the menu bar, select *Run>Isabelle>Isabelle Configurations*.
3. Select *Isabelle for Windows* in the left hand pane, click the *'New Launch Configuration'* button (see Figure 1 in Section 3.1) and provide a name for the configuration: *Isabelle-CML*.
4. In the *Main* tab provide the location of the Isabelle application (for example *C:\Programs\Isabelle2013*, as chosen in Section 2.1). Use the *Browse File System...* button to navigate to the correct location if required, see Figure 8.

**NOTE: do not select a logic at this point**.

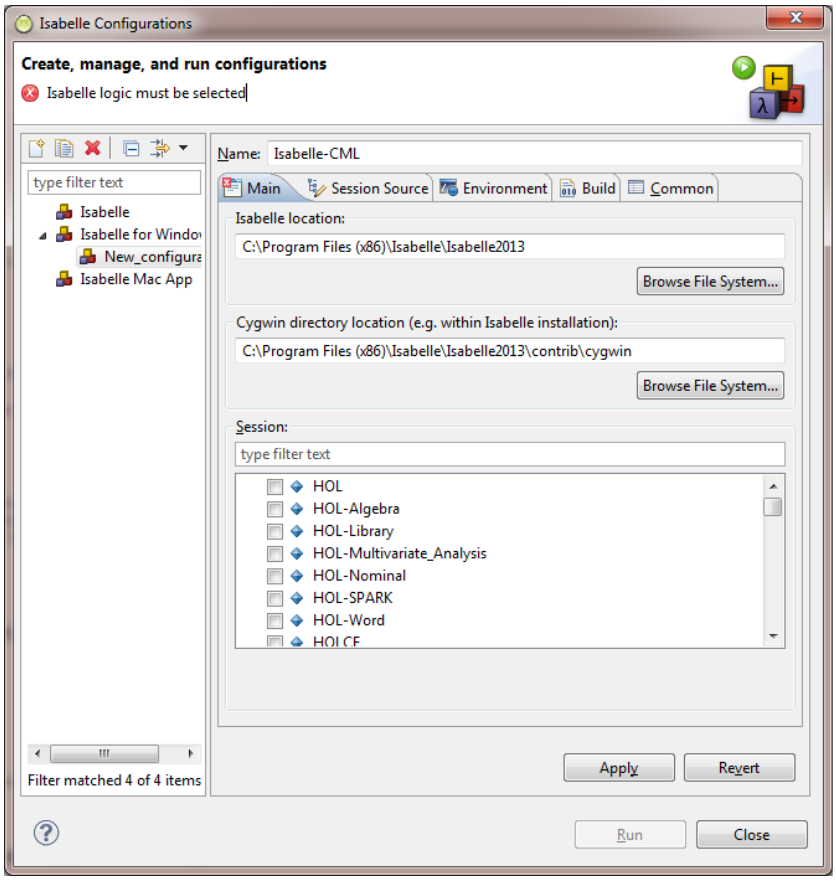


Figure 8: Isabelle configuration in COMPASS Tool – Windows

5. Ensure that the Cygwin directory is automatically populated (Isabelle distributes Cygwin, thus this should be automatically obtained, if not, manually locate a Cygwin installation).

6. For licensing of the Z3 theorem prover used by the Isabelle tool[3], select the *Environment* tab, and click the *'New...'* button. In the *'Name:'* text box enter **Z3_NON_COMMERCIAL**, and in the *'Value:'* text box enter **yes** and click *'Ok'*. Ensure the *'Append environment to the native environment'* option is selected.

7. Select the *Main* tab and in the *Session:* field, choose the *HOL-UTP-CML*

[3]This part of the tool is available free for non-commercial use. For licensing information, see `http://www.microsoftstore.com/store/msuk/en_GB/pdp/Microsoft-Research-Z3-Theorem-Prover/productID.278142500`

logic (there is a filter text box which may help locate the correct logic, see Figure 6).

8. Click the *'Apply'* button to save the configuration, and click the *'Run'* button to start Isabelle. **NOTE:** the first time Isabelle is invoked, several minutes are needed to initialise and build the theories. Subsequent uses of Isabelle will not require this long wait. To monitor progress, click on the button on the bottom right of the tool, as highlighted in Figure 7.

## 3.3 Linux

1. Open the COMPASS Tool application.
2. Configure the COMPASS Tool to use Isabelle – From the menu bar, select *Run>Isabelle>Isabelle Configurations*.
3. Select *Isabelle* in the left hand pane, click the *'New Launch Configuration'* button (see Figure 1 in Section 3.1) and provide a name for the configuration: *Isabelle-CML*.
4. In the *Main* tab provide the location of the Isabelle application (for example */usr/bin/Isabelle2013* as chosen in Section 2.1). Use the *'Browse File System...'* button to navigate to the correct location if required, see Figure 9. **NOTE: do not select a logic at this point**.
5. Select the *Session Source* tab, and click the *'Add external...'* button. Navigate to the location of the utp-isabelle folder extracted in Section 2.2, see Figure 3, and click *'Ok'*.
6. For licensing of the Z3 theorem prover used by the Isabelle tool[4], select the *Environment* tab, and click the *'New...'* button. In the *'Name:'* text box enter **Z3_NON_COMMERCIAL**, and in the *'Value:'* text box enter **yes** and click *'Ok'*. Ensure the *'Append environment to the native environment'* option is selected.
7. Select the *Build* tab, and select the *Build sessions to user home directory* button, see Figure 5.
8. Select the *Main* tab and in the *Session:* field, choose the *HOL-UTP-CML* logic (there is a filter text box which may help locate the correct logic, see

[4]This part of the tool is available free for non-commercial use. For licensing information, see `http://www.microsoftstore.com/store/msuk/en_GB/pdp/Microsoft-Research-Z3-Theorem-Prover/productID.278142500`

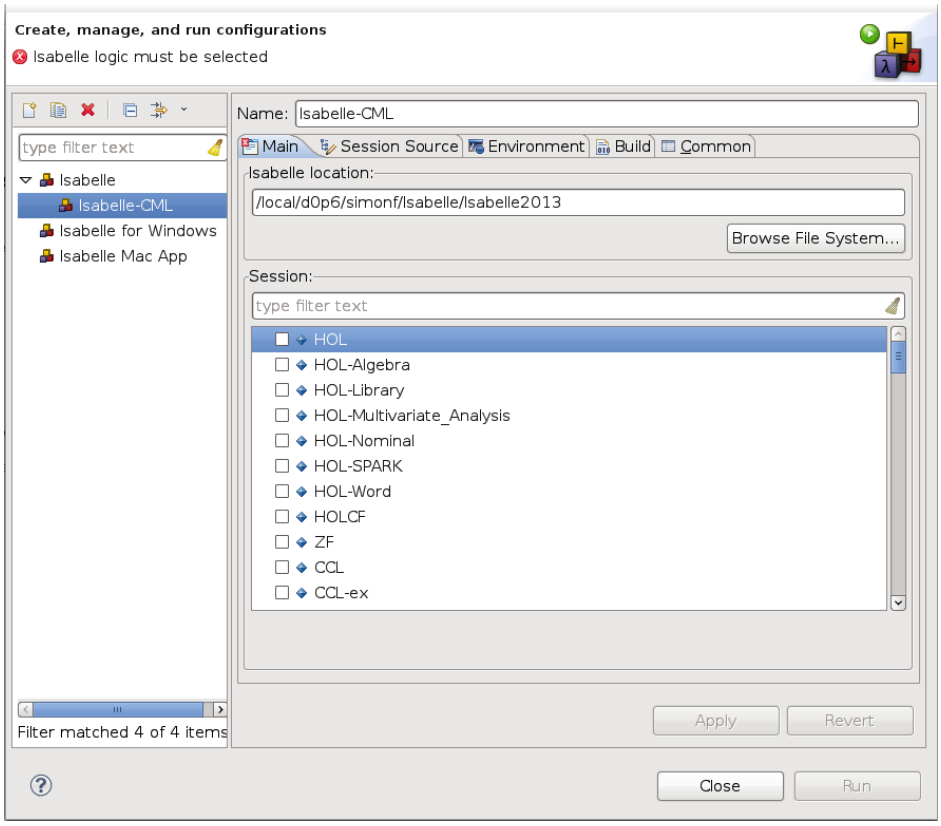


Figure 9: Isabelle configuration in COMPASS Tool – Linux

Figure 6).

9. Click the *'Apply'* button to save the configuration, and click the *'Run'* button to start Isabelle. **NOTE:** the first time Isabelle is invoked, several minutes are needed to initialise and build the theories. Subsequent uses of Isabelle will not require this long wait. To monitor progress, click on the button on the bottom right of the tool, as highlighted in Figure 7.

## 3.4 Updating Theories

Periodically, the UTP/CML theories will be updated. When a new version is available, follow the steps in Section 2.2 to obtain and unpack the newest theories. When this is done, several of the steps described in Section 3.1, 3.2 or 3.3 should be repeated. For all platforms:

1. Open the COMPASS Tool application.

2. Select *Run>Isabelle>Isabelle Configurations* from the menu bar, to begin editting the existing Isabelle configuration.
3. Select *Isabelle* in the left hand pane, select the configuration: *Isabelle-CML*, found under the option corresponding to the correct platform.
4. Select the *Session Source* tab, select the location of the previous utp-isabelle folder and click the *'Remove...'* button.
5. Still on the *Session Source* tab, click the *'Add external...'* button. Navigate to the location of the **new** utp-isabelle folder extracted in Section 2.2.
6. Select the *Main* tab and in the *Session:* field, choose the *HOL-UTP-CML* logic (there is a filter text box which may help locate the correct logic, see Figure 6).
7. Click the *'Apply'* button to save the changes made to the configuration, and click the *'Run'* button to start Isabelle. **NOTE:** the first time Isabelle is invoked with the new theory, several minutes are needed to initialise and build the theories. Subsequent uses of Isabelle will not require this long wait.

## 3.5 Troubleshooting

Error reporting in Isabelle is not always very clear. If errors are encountered, ensure that the instructions have been followed carefully – especially when setting the **Z3_NON_COMMERCIAL** environment variable, (in OS X and Linux) selecting the correct location of the utp-isabelle theory and selecting the correct logic.

More detailed instructions are provided at the Isabelle/Eclipse website, which may be of use:

`http://andriusvelykis.github.io/isabelle-eclipse/getting-started/`

If errors persist, please report them using the COMPASS platform bug tracking facility:

`http://sourceforge.net/p/compassresearch/tickets/`

# 4 Using Isabelle perspective with COMPASS tool

The steps in this section should be followed to begin proving theorems using the Isabelle theorem proving support plugin for the COMPASS tool. The steps enable the user to prove theorems for a specific CML model.

1. With a CML model open, right-click on the model filename in the Project Explorer, and select *CML-THY>Generate Theorem Prover THY*, as shown in Figure 10.

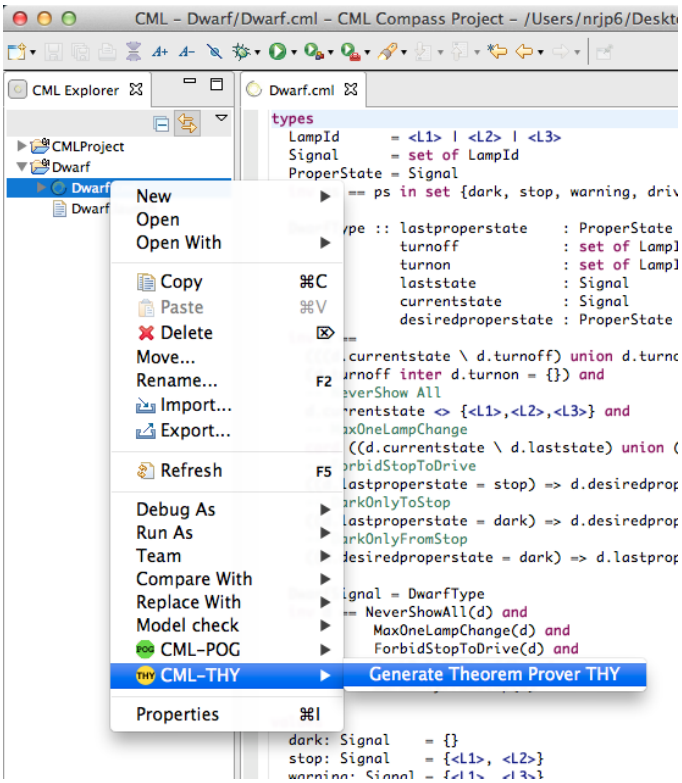


Figure 10: Initiate production of a theory file for a CML model

2. This creates two theory files with the .thy file extension: a model-specific, read-only, file for the CML model (*<modelname>.thy*) and a user-editable file (*<modelname>_User.thy*). These files along with a read-only version of the CML model, are added to a timestamped folder in the *PROJECT> generated>Isabelle* folder of the CML project (see Figure 11). Note – this file is specific to the current state of the model. Any changes made to the CML model will not be reflected in the thy file, and thus the process must be restarted. The generated model .thy file uses a combination of regular

Isabelle syntax, which is described in various Isabelle manuals and tutorials[5], and the Isabelle syntax defined for CML. This Isabelle/CML syntax is described in detail in [FP13].

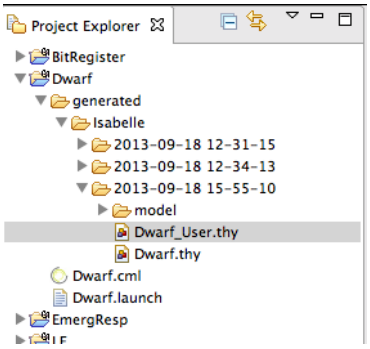


Figure 11: Project explorer with generated .thy files

3. The COMPASS tool should automatically switch to the Isabelle perspective and open the newly generated files. Once open, the Isabelle perspective will look like Figure 12. There are various panes in the perspective as follows:

   **Project Explorer** Similar to the CML perspective – this pane shows the projects created in the user's workspace, and their contents.

   **Theory File Editor** A text editor which enables the user to interact with the theory script and prove theorems, add additional definitions, lemmas and theorems.

   **Theory Outline** This pane provides an outline to the contents of the selected theory file including definitions, functions, lemmas and theorems and may be used to navigate the theory file.

   **Prover Progress** A collection of status bars for the currently open theory files – shows the progress made by Isabelle in proving the scripts in the theory file.

   **Prover Output** A window to report error messages and the status of the goals of selected theorems.

   **Symbol Viewer** A quick method of adding mathematical symbols to a theory file. The user can double-click a symbol which will be added to the proof script.

[5] `http://isabelle.in.tum.de/documentation.html`

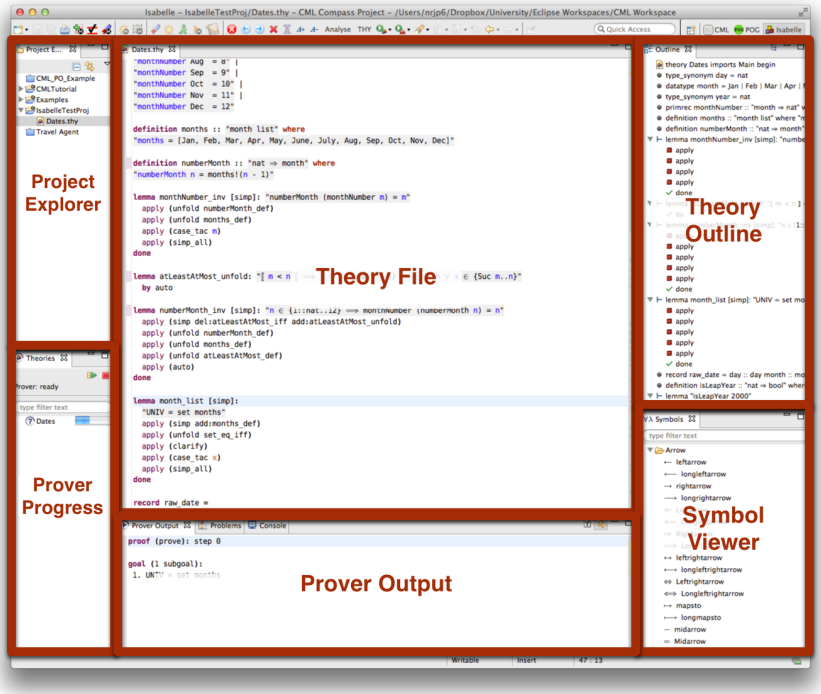


Figure 12: Overview of Isabelle perspective in COMPASS Tool

4. If the Isabelle perspective is not opened automatically, or the perspective needs changing manually, then select the icon labelled **b** in Figure 13, and then select *Isabelle* and then *ok*. If the perspective has been used previously, then select the Isabelle perspective using the button labelled **c** in Figure 13.

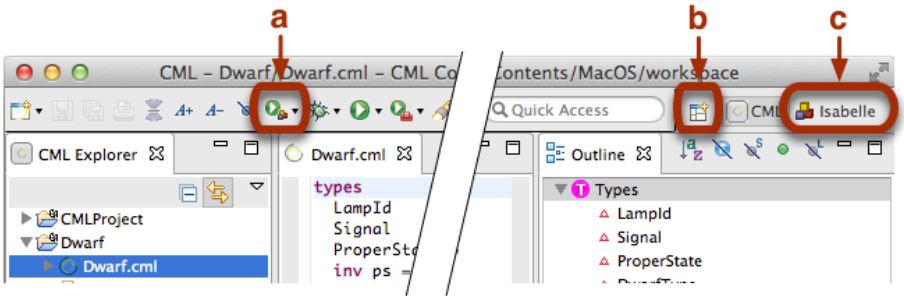


Figure 13: Running Isabelle and selecting Isabelle perspective

5. If Isabelle is not already running, press the button labelled **a** in Figure 13. This will run the most recent Isabelle configuration (defined in Section 3).

If a different configuration is required, use the down arrow to select the required configuration. If there is already an instance of Isabelle running, an error message will appear, as in Figure 14. This can be safely dismissed.

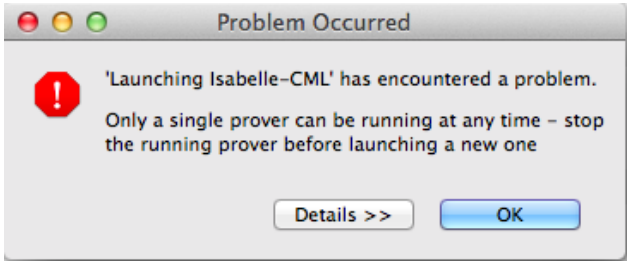


Figure 14: Overview of Isabelle perspective in COMPASS Tool

6. To view or edit those theory files created in step 1, navigate to their location in the project explorer and double click on the file name. Using the theory file editor pane, theorems and lemmas may be defined and proven. The theory editor of Isabelle/Eclipse provides an interactive, asynchronous method for theorem proving, similar to the jEdit interface distributed with Isabelle. The theory file is submitted to Isabelle and results are reported asynchronously in the editor and prover output panes. The editor has syntax highlighting for the Isabelle syntax[6] and problems are marked and displayed in the output pane.

In the next section, we use the steps defined here to use the Isabelle perspective to prove lemmas related to an example CML model.

[6]It is beyond the scope of this document to describe the Isabelle syntax – interested readers are directed to the tutorials, available at `http://isabelle.in.tum.de`.

# 5 Proving CML Theorems

In this section, we provide a brief overview to theorem proving in the COMPASS tool. As proving theorems about a CML model in Isabelle is performed in much the same way as normal theorem proving in Isabelle, the interest reader should refer to tutorials on theorem proving with Isabelle for more details[7].

To illustrate the process of proving theorems, we use an example introduced in Part B of this deliverable [FP13] – the Dwarf signal controller. In Figure 15, the original CML model (*Dwarf.cml*) and the generated .thy file (*Dwarf.thy*) are shown in the COMPASS tool. The process detailed in Section 4 was used to generate the .thy file. The generated file is set as read-only by the tool – and therefore should not be edited. The generated .thy file uses a combination of regular Isabelle syntax, which is described in various Isabelle manuals and tutorials[8], and the Isabelle syntax defined for CML. This Isabelle/CML syntax is described in detail in [FP13].

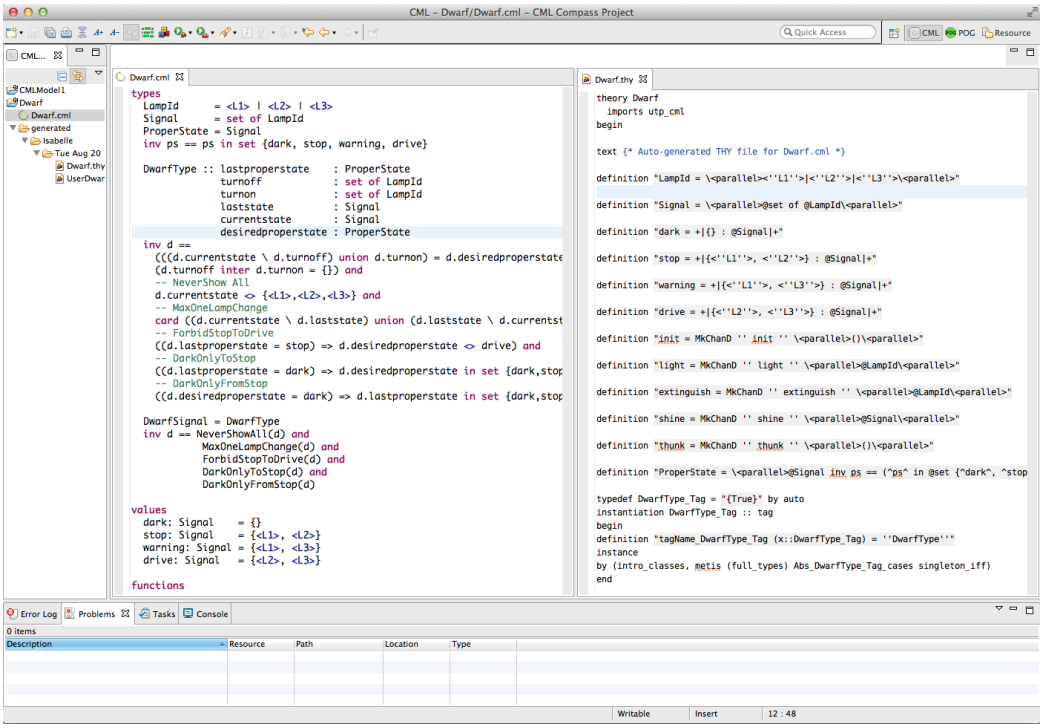


Figure 15: Example Dwarf CML model and generated .thy file

[7] http://isabelle.in.tum.de/documentation.html
[8] http://isabelle.in.tum.de/documentation.html

In the corresponding generated timestamped Isabelle directory, a user-editable .thy file is produced – in this example, that file is named *Dwarf_User.thy*. This file imports the utp_cml theory and the generated Dwarf model theory. This file is shown in Figure 16.

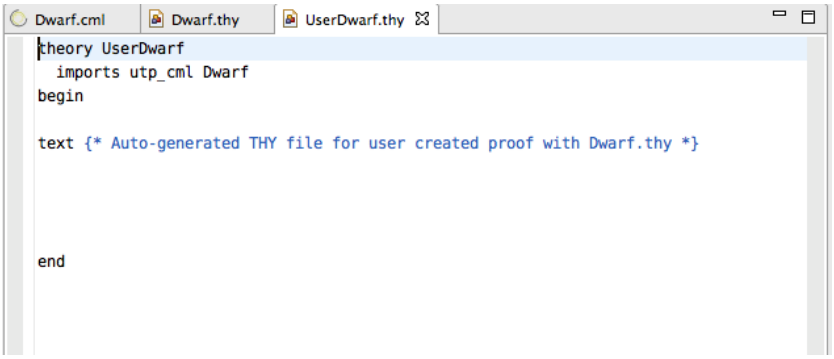


Figure 16: Initial user-editable Dwarf_User.thy file

Switching to the Isabelle perspective, and running the Isabelle configuration, we may start stating and proving theorems and lemmas. In Figure 17, we begin to prove some of those theorems introduced in [FP13]. These theorems, named *nsa*, *molc* and *fstd*, are added to the user-editable theory file *Dwarf_User.thy*.

The theorems use a combination of regular Isabelle syntax (both using apply-style scripts and the Isar syntax) which is described in various Isabelle manuals and tutorials[9], and the Isabelle syntax defined for CML. This Isabelle/CML syntax is described in detail in [FP13]. Each theorem has the *oops* keyword below. This signifies that we aim to prove the theorem at a later point and do not yet provide any proof.

In the theory outline pane, shown in more detail in Figure 18, the oops keyword is specified, and the box icon denotes the proof is not complete. Also, no prover output is shown when selecting an area after the proofs. If the user wants more information about the theorem, this is available by placing the editor cursor on the theorem.

In Figure 19, we discharge these theorems. The theorems are all simply proved using the *cml_tac* proof tactic. The tactic is applied by using the line *"by (cml_tac)"* on the line below the theorem. This applies rules and tactics defined in the isabelle-utp UTP and CML theories imported during the initial setup of the theorem prover. This tactic is described in more detail in Part B of this deliverable [FP13].

[9] `http://isabelle.in.tum.de/documentation.html`

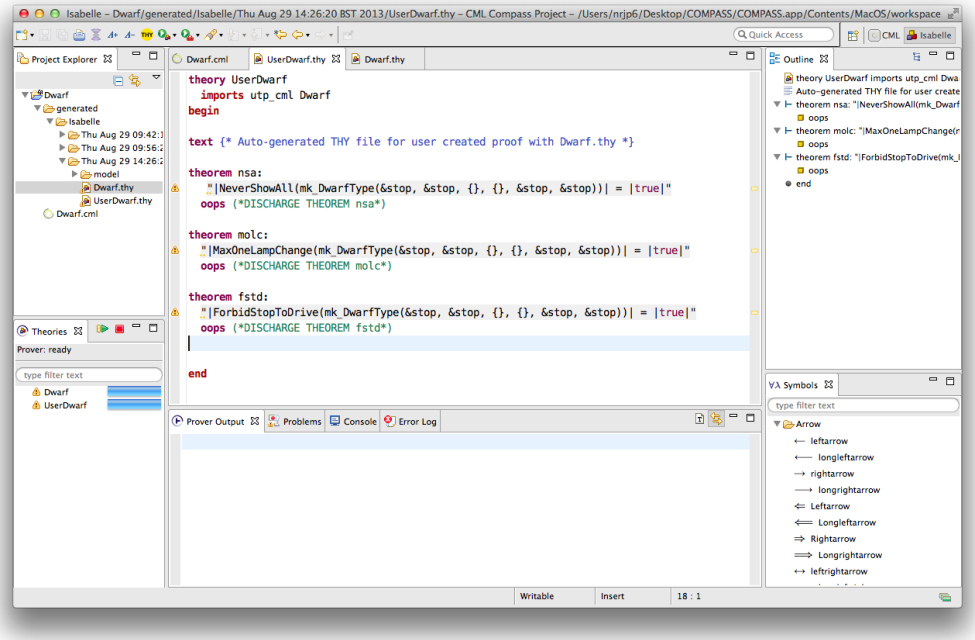


Figure 17: Unproved theorems in Isabelle perspective

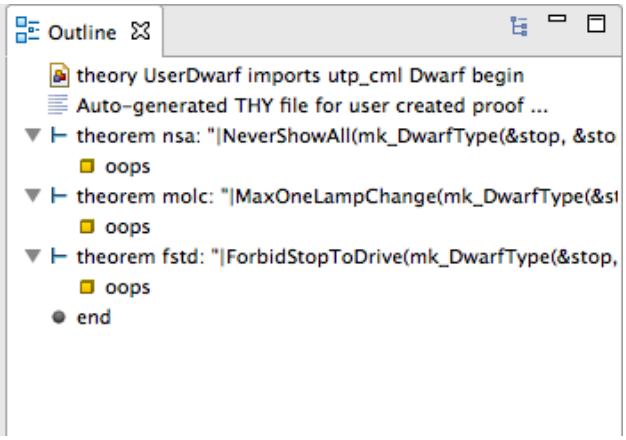


Figure 18: Proof outline of unproved theorems Isabelle perspective

As can be seen in the proof outline pane, shown in more detail in Figure 20, each theorem now has a green tick signifying the theorem has been discharged. Proof output is also shown in the output pane providing some details on the proof.

It is beyond the scope of this document to provide detailed descriptions of theorem proving, using the Isabelle tool, or to provide a tutorial on it's use. We therefore

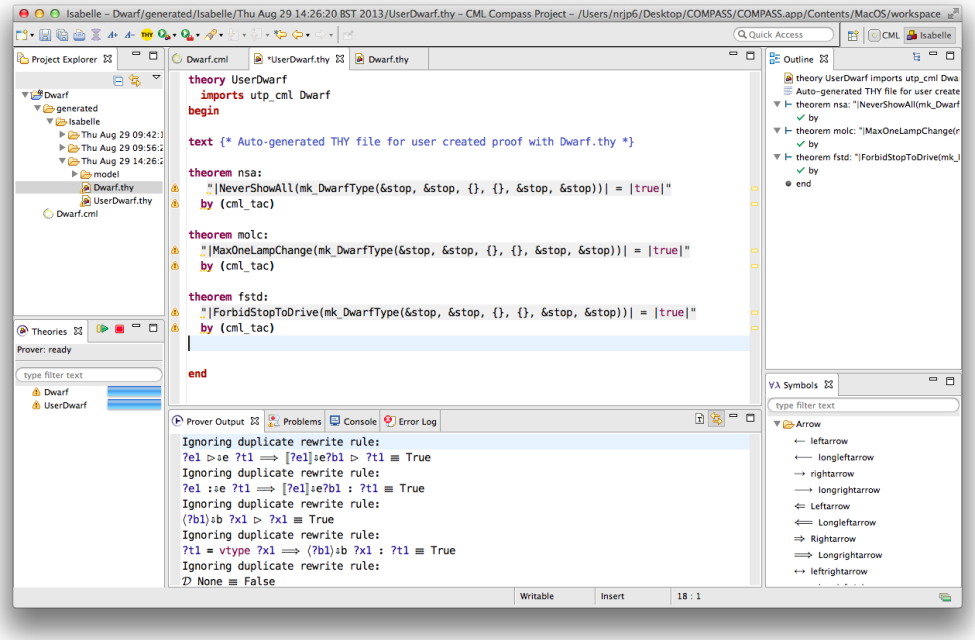


Figure 19: Discharged theorems in Isabelle perspective

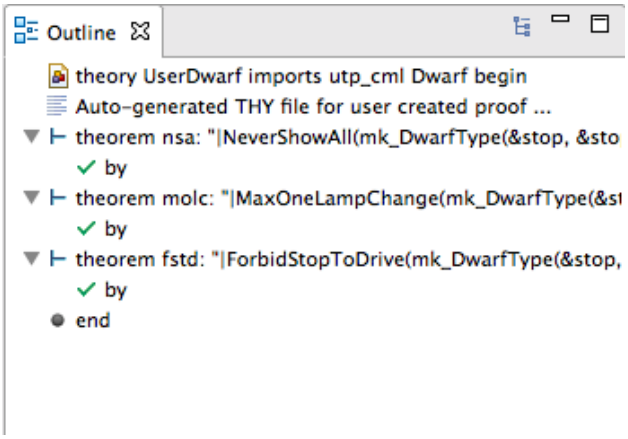


Figure 20: Proof outline of proved theorems Isabelle perspective

recommend that interested parties should read this deliverable in conjunction with tutorials on Isabelle and proving in the Isabelle tool, available on the Isabelle website[10].

[10]http://isabelle.in.tum.de/documentation.html

# 6 Conclusions

This document has given an introduction to using Isabelle in the COMPASS tool to perform theorem proving with CML models. The document is not able to provide a thorough introduction to proving using Isabelle, therefore the interested reader should refer to the Isabelle website[11] for extensive tutorial and exercise literature on proving in Isabelle and the underlying fundamentals of Isabelle. Whilst the UTP logic used in proving in CML is not used in the literature at this website, the general lessons are applicable.

The companion deliverable D33.2b provides more technical insight into the development of the theorem proving support plugin, and should be read in conjunction to this user manual for a greater understanding of the underlying theories used.

[11] http://isabelle.in.tum.de/

# References

[BGW12] Jeremy Bryans, Andy Galloway, and Jim Woodcock. CML definition 1. Technical report, COMPASS Deliverable, D23.2, September 2012.

[CMLC13] Joey W. Coleman, Anders Kaels Malmos, Rasmus Lauritsen, and Luís D. Couto. Second release of the COMPASS tool — user manual. Technical report, COMPASS Deliverable, D31.2a, January 2013.

[Col13] Joey W. Coleman. Second release of the COMPASS tool — tool grammar reference. Technical report, COMPASS Deliverable, D31.2c, January 2013.

[FP13] Simon Foster and Richard J. Payne. Theorem proving support - developers manual. Technical report, COMPASS Deliverable, D33.2b, September 2013.

[WCF+12] J. Woodcock, A. Cavalcanti, J. Fitzgerald, P. Larsen, A. Miyazawa, and S. Perry. Features of CML: a Formal Modelling Language for Systems of Systems. In *Proceedings of the 7th International Conference on System of System Engineering*. IEEE, July 2012.