Collins CASE TA2 Attestation Transform

|  |
| --- |
| To illustrate the Attestation transform, we use a simple producer-consumer example model, which can be found here:  https://github.com/loonwerks/CASE/tree/master/TA2/Model\_Transformations/Attestation/Simple\_Example  Two AADL packages are included:   * Attestation.aadl – This is the initial model. * CASE\_Requirements.aadl – This is the package containing the requirement (in the form of a Resolute claim) that drives the attestation transform.   The Attestation transform can also be performed on the CASE Phase 1 UAV example model. Three versions of the model are available for reference:   * Initial model – This is the Phase 1 UAV model that includes an imported cyber requirement, which drives the attestation of the source of incoming messages to the FlightPlanner component. The Initial model can be found here:   [https://github.com/loonwerks/CASE/tree/master/TA2/Model\_Transformations/Attestation/ UAV\_Example/Initial\_Model](https://github.com/loonwerks/CASE/tree/master/TA2/Model_Transformations/Attestation/%20UAV_Example/Initial_Model)   * Transformed model – This is the Phase 1 UAV model after the Attestation transform has been applied. The Transformed model can be found here:   [https://github.com/loonwerks/CASE/tree/master/TA2/Model\_Transformations/Attestation/ UAV\_Example/Transformed\_Model](https://github.com/loonwerks/CASE/tree/master/TA2/Model_Transformations/Attestation/%20UAV_Example/Transformed_Model)   * Test model – This is the Phase 1 UAV model containing several software implementations for testing the correctness of the Resolute evaluation on the Attestation transform. The Test model can be found here:   [https://github.com/loonwerks/CASE/tree/master/TA2/Model\_Transformations/Attestation/ UAV\_Example/Test\_Model](https://github.com/loonwerks/CASE/tree/master/TA2/Model_Transformations/Attestation/%20UAV_Example/Test_Model) |

A CASE Attestation Manager is added to a communication driver component to ensure that only messages from trustworthy sources are accepted. Only components with the CASE\_Properties::COMP\_TYPE = COMM\_DRIVER property association can have an Attestation Manager connected to it, and only one Attestation Manager may be connected to a communication driver. All outgoing connections from the communication driver will pass through the Attestation Manager. The Attestation Manager component type that is inserted into the model will be the same component type as the communication driver.

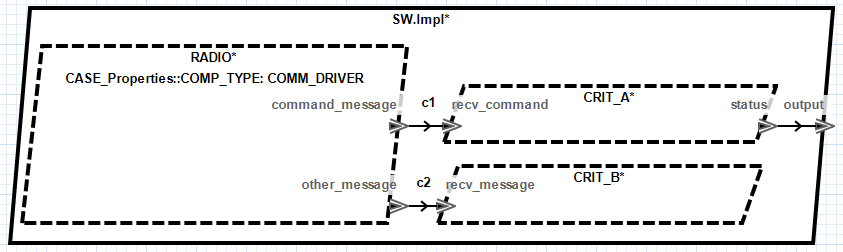


Figure 1. Initial model.

The Attestation Manager is added to the model by selecting a communication driver subcomponent in a component implementation and clicking the CASE 🡪 Cyber Resiliency 🡪 Model Transformations 🡪 Add Attestation Manager… menu item. A wizard will appear, as shown in Figure 2, enabling the user to customize the Attestation Manager.

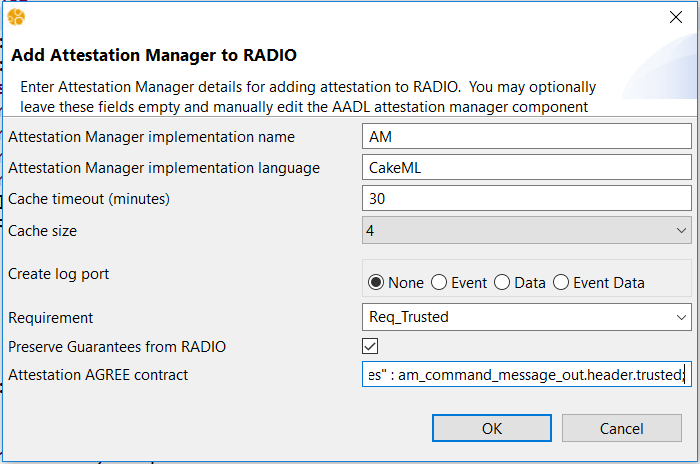


Figure 2. Add Attestation Manager wizard.

The Attestation transform will create a special CASE\_AttestationManager AADL component type and implementation, and insert them into the model. It will then instantiate the CASE\_AttestationManager implementation as a subcomponent in the implementation containing the selected communication driver. The user may provide a name for the attestation manager subcomponent, or use the default. If the field is left blank, the default name will be used. Note that if the specified name already exists, a number will be appended to the name to make it unique within the containing component implementation.

By default the CASE attestation manager will drop any messages that do not originate from trusted sources, and no record of the malformed message will be retained. If the user wishes to log the event, an additional log port can be added to the filter. The user will need to specify the AADL port type (Event, Data, or EventData) and it will be up to the user to connect the log port to an appropriate “logger” component.

The requirement drop-down box lists all of the cyber-requirements that have been imported from TA1 tools. By specifying the cyber requirement that drives the attestation transform, the appropriate assurance argument can be constructed for demonstrating the requirement was addressed correctly. A requirement does not need to be selected to insert the attestation manager, but it is highly recommended for construction of the proper system assurance case.

Finally, the user may provide an AGREE *guarantee* statement, which is a formal property the attestation manager asserts to always be true as long as stated assumptions on the environment are valid. Specifying such a property is typically done by referring to the outgoing message on the attestation manager’s output port. The message type will be the same as the communication driver component’s output port. Within the AGREE statement, the attestation manager output port name can be referred to by *am\_<Comm\_Driver\_Feature\_Name>\_out*. For the example in Figure 1, if the message header on connection c1 has a field to indicate that the message source is trusted, such as on line 16 of the CASE\_Model\_Transformations.aadl package (see Figure 3):

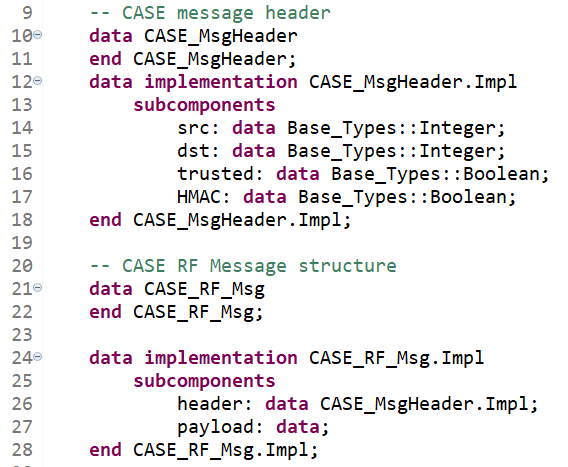


Figure 3. RF message definition in CASE\_Model\_Transformations.aadl.

The AGREE statement will then be:

guarantee Req\_Trusted\_Attestation "Only messages from trusted sources shall be permitted" : am\_command\_message\_out.header.trusted;

Note that no syntax validation is performed on the AGREE statement. If it is malformed, it may not be imported into the model properly.

Clicking the OK button on the wizard will insert the CASE\_AttestationManager and extended communication driver into the model, as shown in Figure 4 and Figure 5.

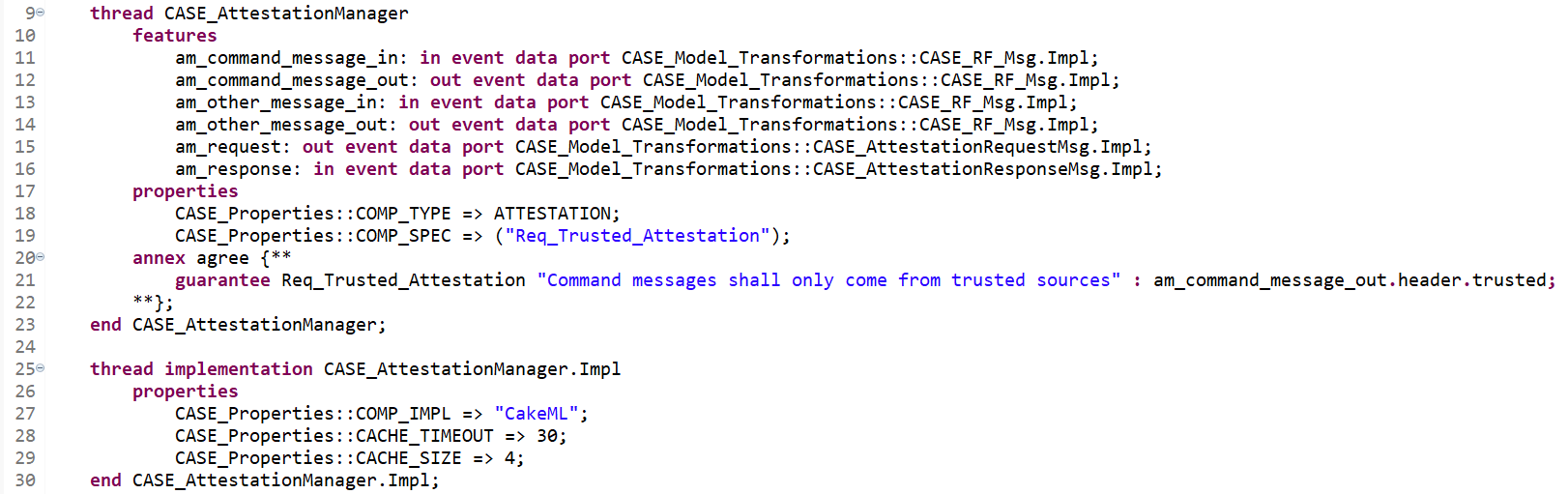


Figure 4. Line 9: CASE\_AttestationManager component type; Line 25: CASE\_AttestationManager component implementation.

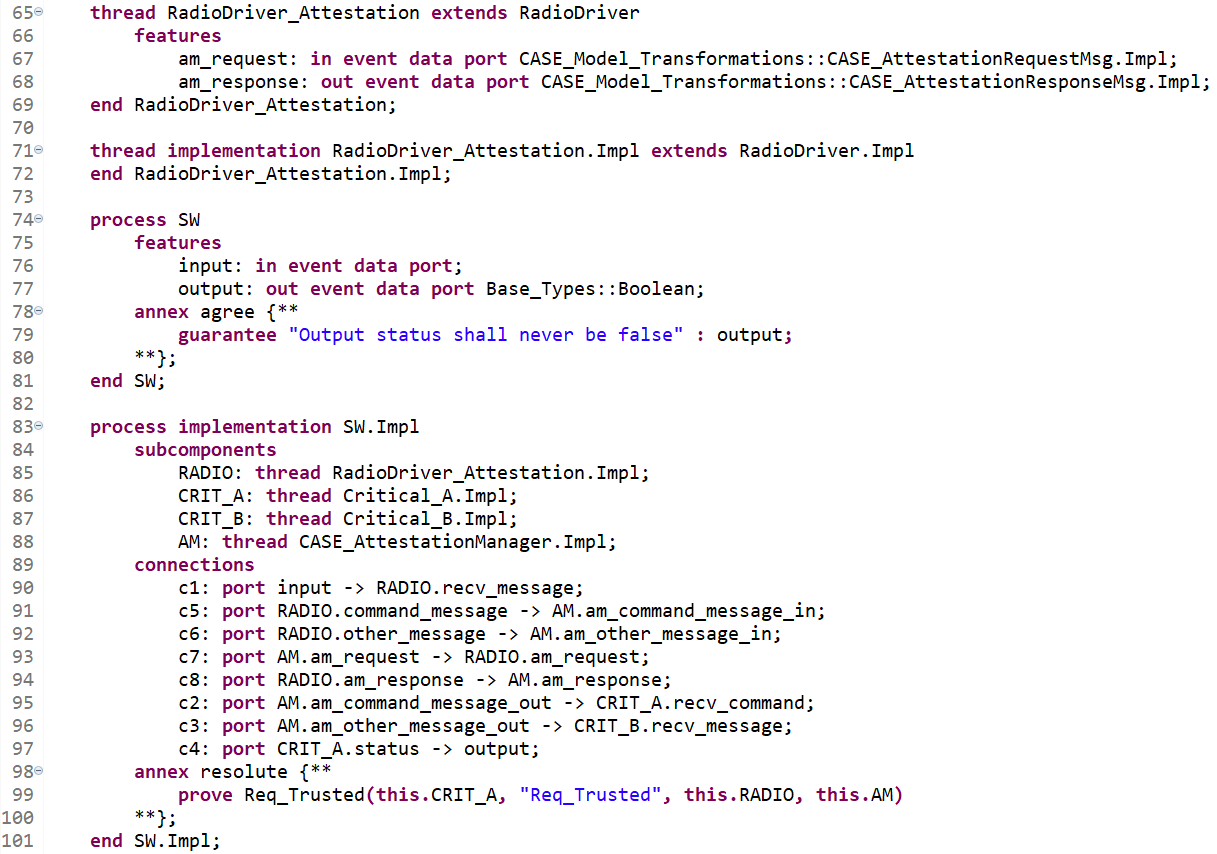


Figure 5. Line 65: Extended communication driver component; Line 88: Attestation Manager subcomponent; Lines 91-96: Attestation Manager connections; Line 99: updated assurance claim call.

Note that for every internal outgoing connection from the communication driver, a corresponding input and output port is created in the attestation manager. The Attestation transform also adds two connections between the Attestation Manager and the communication driver to perform the attestation with the message source. In addition, two corresponding response and request ports are added for communication with the message sender. These ports are intentionally left unconnected. It is up to the user to connect them to a corresponding attestation manager on the system of the message sender, if contained in the model. Because the communication driver implementation may be instantiated in other parts of the system, a new communication driver with the additional attestation ports is created that extends the original communication driver.

### Design Assurance

It is crucial to have evidence of design correctness both at the time the model transformation is performed, and at any time up through system build. Resolute provides that assurance via augmentation of the requirement with assurance subclaims as model transformations are performed.

When a requirement is imported from a TA1 tool it will be placed in the CASE\_Requirements package as a Resolute claim, as shown in Figure 6.

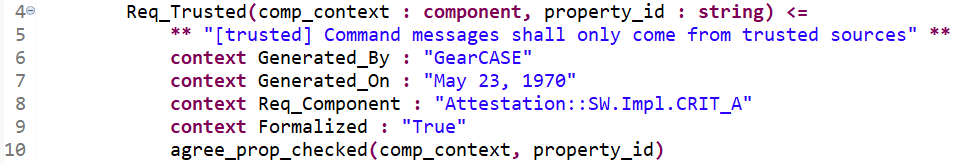


Figure 6. Requirement imported from a TA1 tool.

Initially, there is not much for Resolute to check because the requirement hasn’t yet been addressed in the design. All Resolute can do in this example is check that AGREE analysis was performed. Note that Resolute uses a separate plugin called AgreeCheck to determine if AGREE analysis was performed. AgreeCheck is included with Resolute, but requires initial user configuration. In order to successfully use AgreeCheck, "Generate property analysis log" must be checked in the AGREE Analysis preferences, and a log file pathname must be specified. The AGREE Analysis preferences can be accessed by selecting Window → Preferences from the main menu, expanding the Agree node on the left-hand side of the preference window, and selecting Analysis.

Once the Attestation transform is applied, the requirement is updated with an additional check to make, which reflects the addition of the attestation manager component, as shown in Figure 7.

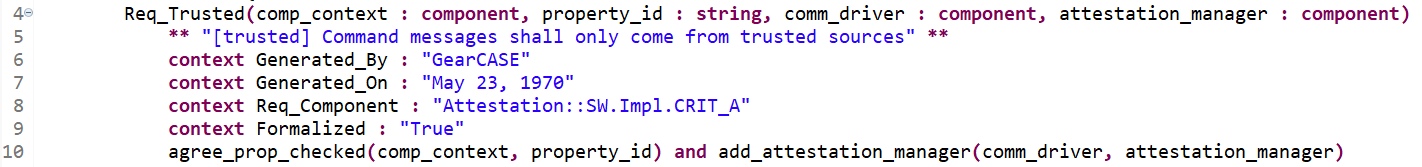


Figure 7. Modified requirement after Attestation transform.

The addition of the add\_attestation\_manager() call on line 10 provides Resolute with additional checks to make to ensure the requirement was addressed correctly. In this case, add\_attestation\_manager() is included in the CASE\_Model\_Transformations library and consists of two subclaims:

* attestation\_manager\_exists() – Checks that the attestation manager component is present in the model
* attestation\_manager\_not\_bypassed() – Checks that there are no connections in the model that bypass the attestation manager

To check whether the requirement has been correctly addressed in the design, select the containing component implementation (SW.Impl on line 83 in Attestation.aadl) and select Analyses 🡪 Resolute from the main menubar. The Resolute output will appear in the output pane, as shown in Figure 8.

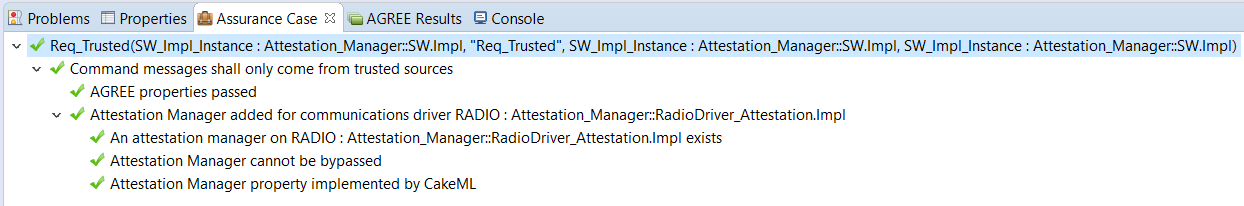


Figure 8. A passing Resolute analysis.