**MBSE Modeling Guidelines**

**With**

**SysML and Rhapsody**

V 1.0

December 23, 2020

Prepared by

Dr. Bruce Powel Douglass, Ph.D.

A Priori Systems

[www.bruce-douglass.com](http://www.bruce-douglass.com)

Table of Contents

Contents

[Overview 4](#_Toc59654233)

[Tooling and Languages 4](#_Toc59654234)

[Definitions and Acronyms 4](#_Toc59654235)

[Syntactic Standards 6](#_Toc59654236)

[General Modeling Standards 6](#_Toc59654237)

[Model Organization 7](#_Toc59654238)

[Federating Rhapsody models 7](#_Toc59654239)

[Naming Conventions 11](#_Toc59654240)

[Basic Naming convention 11](#_Toc59654241)

[General Diagramming Conventions 14](#_Toc59654242)

[Every diagram shall have a singular mission 14](#_Toc59654243)

[Other diagramming conventions 16](#_Toc59654244)

[Block Definition Diagrams (BDDs) 17](#_Toc59654245)

[Content 17](#_Toc59654246)

[Block and Parts 18](#_Toc59654247)

[Interfaces 18](#_Toc59654248)

[Interface Blocks and Ports 18](#_Toc59654249)

[Relations 19](#_Toc59654250)

[Internal Block Diagrams (IBDs) 21](#_Toc59654251)

[Use Case Diagrams 21](#_Toc59654252)

[Use Cases 21](#_Toc59654253)

[Actors 23](#_Toc59654254)

[Relations 23](#_Toc59654255)

[Requirements Diagrams 23](#_Toc59654256)

[Relations 24](#_Toc59654257)

[Requirements Tables 24](#_Toc59654258)

[Matrices 24](#_Toc59654259)

[Sequence Diagrams 24](#_Toc59654260)

[Activity Diagrams 27](#_Toc59654261)

[State Diagrams 28](#_Toc59654262)

[States 28](#_Toc59654263)

[Actions 32](#_Toc59654264)

[Guards 33](#_Toc59654265)

[Submachines 33](#_Toc59654266)

[Parametric Diagrams 33](#_Toc59654267)

[Parametrics for architectural analysis 34](#_Toc59654268)

[Semantic Standards: Using SysML 35](#_Toc59654269)

[Model Overview Diagram 35](#_Toc59654270)

[Modeling Systems Architecture Context 36](#_Toc59654271)

[Modeling Systems Architecture Behavior 39](#_Toc59654272)

[Modeling Data Schema 39](#_Toc59654273)

[Defining a Named Constant 40](#_Toc59654274)

[Modeling Trade Studies 41](#_Toc59654275)

[Relating to ASPICE and ISO 26262 42](#_Toc59654276)

[Safety Profile 42](#_Toc59654277)

[Generating Reports 42](#_Toc59654278)

[References 44](#_Toc59654279)

# Overview

This document is to provide a set of principles and specific guidance for the development of Model-Based Systems Engineering (MBSE) in SysML with the Rhapsody tool.

## Tooling and Languages

The Rhapsody tool shall be used to model the requirements, architecture, interfaces and other system information. Other tools, such as Simulink, may be used as well, but their use falls outside the guidance provided by this Guideline. The version of Rhapsody, at the time of this writing, is 8.4, although it is anticipated that the tool will be upgraded to later versions over time.

The systems model will be specified in the SysML Language. The actual language addressed in this Guidelines includes both the C and C++ programming languages.

## Definitions and Acronyms

BDD – Block Definition Diagram; a structural diagram type defined in the SysML, representing blocks and types, their structural properties, and their relations.

Class Diagram –a structural diagram type defined in the UML, representing classes and types, their structural properties, and their relations.

Composition Architecture – a model of the internal structure of a System in terms of its large-scale classes or blocks, their properties, and their relations.

Connected Architecture – a model of the internal structure of a System in terms of instances or parts instantiated from elements of its Composition Architecture

Connected Context – a model of the system environment in terms of instances or parts instantiated from the System and its related Actors.

Context Architecture – a model of how the system fits into its environment, in terms of the actors to which it connects and the relations among those elements.

Data Schema – a model representing information, its important properties and its relations. Data schemas are represented using BDDs in SysML and Class Diagrams or OMDs in UML.

Forced Closure Rule – The set of actions executing when a transition is taken completes when the state is entered; this includes exit, transition, and entry actions.

IBD – Internal Block Diagram; a structural diagram type defined in the SysML, representing instances (aka Parts) and their relations.

Instance – a run-time occurrence of a block or class. Also known as a *part* or *object.*

Magic number – a literal numeric value that appears in a design without documentation, justification, or rationale.

MBSE – Model Based Systems Engineering; the use of models as the primary work products to capture, represent, and analyze systems engineering data. The primary language used for MBSE is SysML.

MDD – Model-Driven Development; the use of models to capture and represent software architecture and design.

Model Overview Diagram – a diagram used to explain the purpose, scope, and organization of a model

OMD – Object Model Diagram; a Rhapsody-specific structural diagram which is basically a UML class diagram

Package Diagram – a diagram whose primary purpose is to show model organization via packages, their relations, and their content.

Parametric diagram – a SysML diagram that specializes an Internal Block Diagram. This diagram is used to show the relation between values and constraint properties.

Part – see Instance.

Rhapsody – a powerful UML and SysML modeling tool.

Scenario – a particular sequence of interactions between a set of elements, often used to model interactions during use case analysis

Sequence diagram – an interaction diagram in UML and SysML used to model scenarios and test cases.

Structure Diagram – a kind of structural diagram that shows instances, their properties, and their relations in a UML model

SysML – the Systems Modeling Language, a profile of the UML standard used to model systems concepts

Type Architecture – a model of the structural elements of a set of elements, typically capture in a UML Class or OMD diagram or a SysML Block diagram

UML – the Unified Modeling Language, the pre-eminent standard for software modeling, and the basis of the SysML modeling language.

Use Case – a collection of system actions that represents a coherent usage of a system.

# Syntactic Standards

## General Modeling Standards

* All important model elements shall have a comment that describes why the element exists, how it contributes to the model, general usage of the element, and constraints on that element. This applies to (description includes standard fields expected for the kind of element). Note: Safety metadata is missing from the description because, where appropriate, it will be specified by applying stereotypes from the *Safety Profile*.
  + Projects
    - **Purpose**
    - **Description**
  + Diagrams
    - **Mission**
  + Blocks
    - **Purpose**:
    - **Represents**:
    - **Roles**:
    - **Description**:
    - **Security Constraints**:
    - **Pre-conditions**:
    - **Post-conditions**:
    - **Invariants**:
  + Value properties   
    Note: the value property metadata valid range, units, accuracy, precision, and fidelity, disallowed values, etc. may be supplied via the application of stereotypes from the *Safety Profile.*
    - **Purpose**:
    - **Represents**:
    - **Roles**:
    - **Description**:
    - **Security Constraints**:
    - **Pre-conditions**:
    - **Post-conditions**:
    - **Invariants**
  + Value types and units  
    Note: the value property metadata valid range, units, accuracy, precision, and fidelity, disallowed values, etc. may be supplied via the application of stereotypes from the *Safety Profile*.
    - **Purpose**:
    - **Represents**:
    - **Description**:
    - **Security Constraints**:
    - **Pre-conditions**:
    - **Post-conditions**:
    - **Invariants**
  + Operations
    - **Purpose**:
    - **Processing performed**:
    - **Algorithm/pattern**:
    - **Return value constraints**:
    - **Security constraints**:
    - **Pre-conditions**:
    - **Post-condition**:
    - **Timing constraints**:
  + Actors
    - **Purpose**:
    - **Represents**:
    - **Roles**:
    - **Description**:
    - **Security Constraints**:
    - **Pre-conditions**:
    - **Post-conditions**:
    - **Invariants**:
  + Use cases
    - **Purpose**:
    - **Processing performed**:
    - **Algorithm/pattern**:
    - **Return value constraints**:
    - **Security constraints**:
    - **Pre-conditions**:
    - **Post-condition**:
    - **Timing constraints**:
* Some of these properties may be omitted if inapplicable OR if captured as metadata in stereotype tags

## Model Organization

### Federating Rhapsody models

Basic federation organization shall be:

* One systems requirements & architecture model as shown in Figure 1.
  + Note: If the Systems model is large, it can be split into multiple models
* As can be seen, this would contain the use cases, requirements and architecture of the overall system.
* The recommended SE Model organization is shown in Figure 2.
* One model per subsystem (Figure 3). This would contain the model components for an individual subsystem.
  + One package shall contain the requirements, use cases, and other specification elements for the model, imported from the SE model.
  + One package shall represent the deployment architecture (electronics, mechanical, software allocations) of the subsystem under development
  + One package shall represent the software aspects and is further decomposed.
  + Referenced packages from the Shared Model permit access to shared data and interface specifications
  + Note: Large subsystem models may be broken up into multiple models.
* One (occasionally more) shared model containing common classes, interfaces, and types (Figure 4)

When transitioning from systems engineering model to the subsystem (including the software) models, the SE model organization shall provide a package for the specification of each subsystem, as shown in Figure 1

* The subsystem specifications in the SE model is organized as one package per subsystem contained by the Architectural Design package
* The subsystem model begins by importing the relevant subsystem specification package from the system SE model
  + The subsystem spec package is added *by value* (“as unit” in Rhapsody)
* The shared packages are added into the subsystem models (aka “client models”) *by reference* so that changes to those packages are reflected in the client models when they are loaded

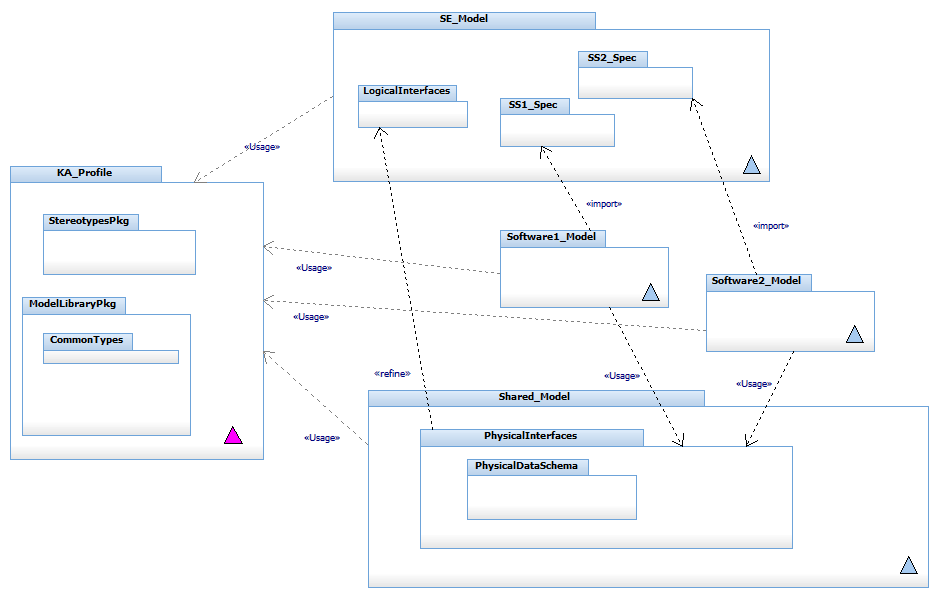


Figure 1: Recommended Model Organization Set

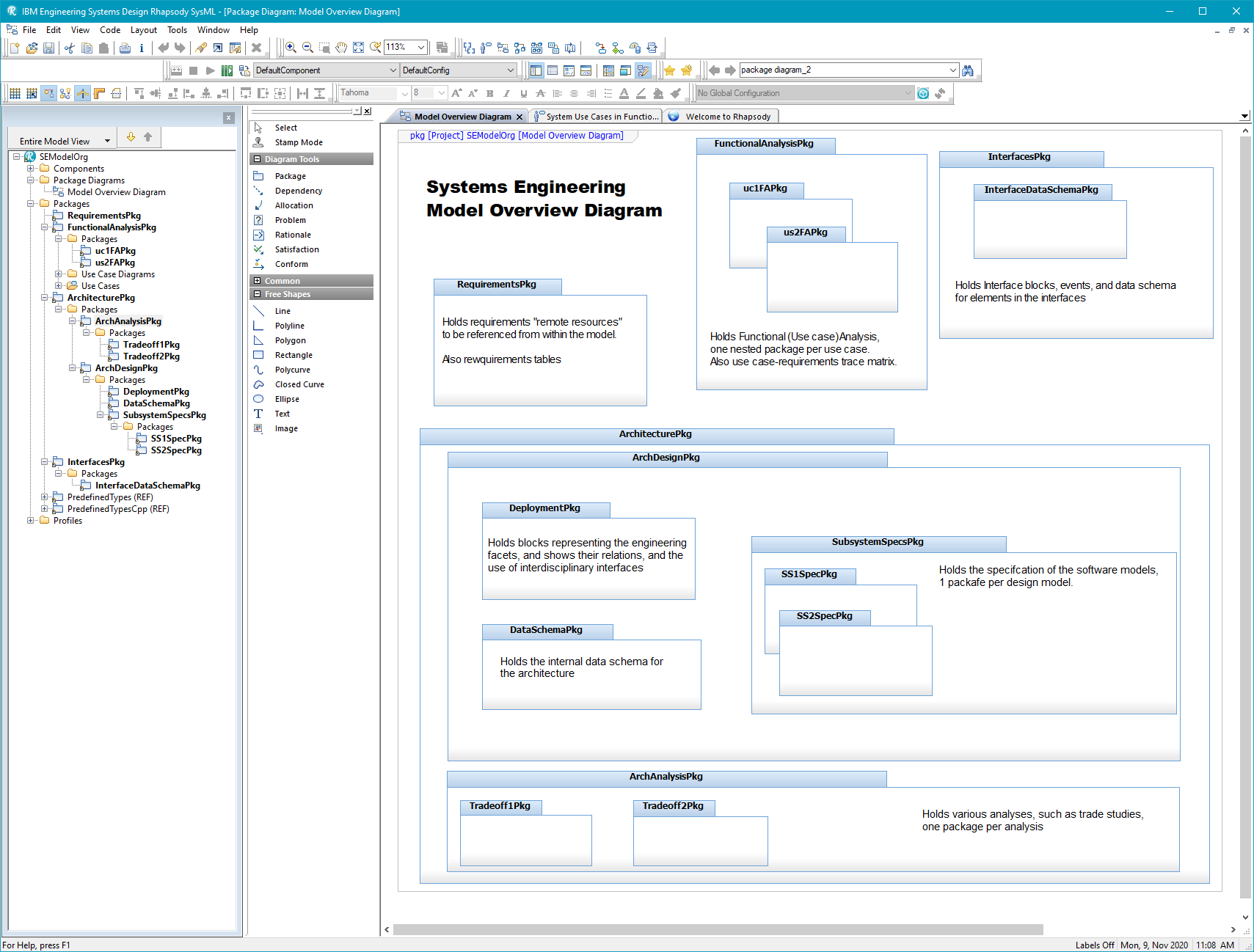


Figure 2: SE Model Organization

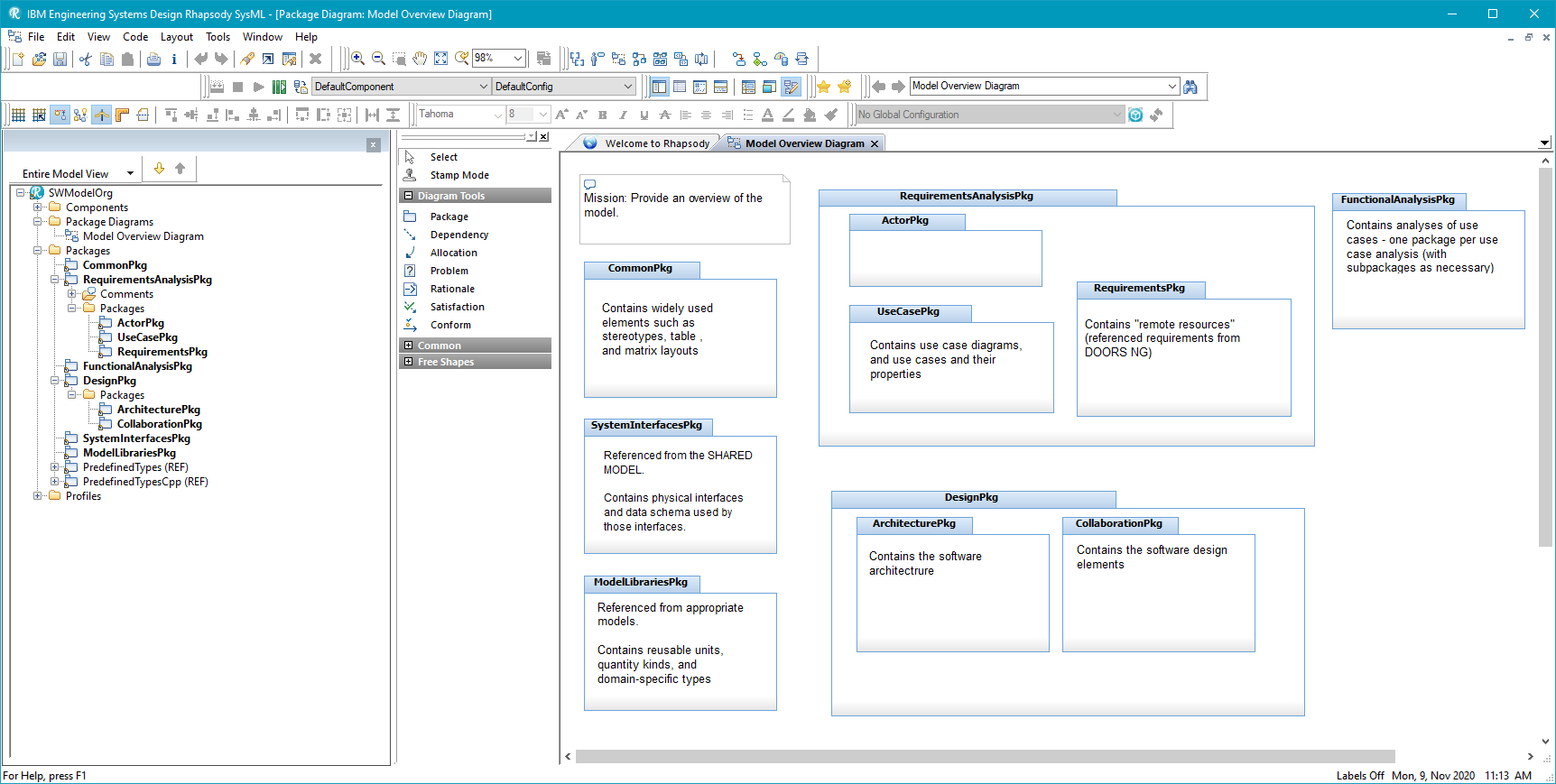


Figure 3: Software Model Organization

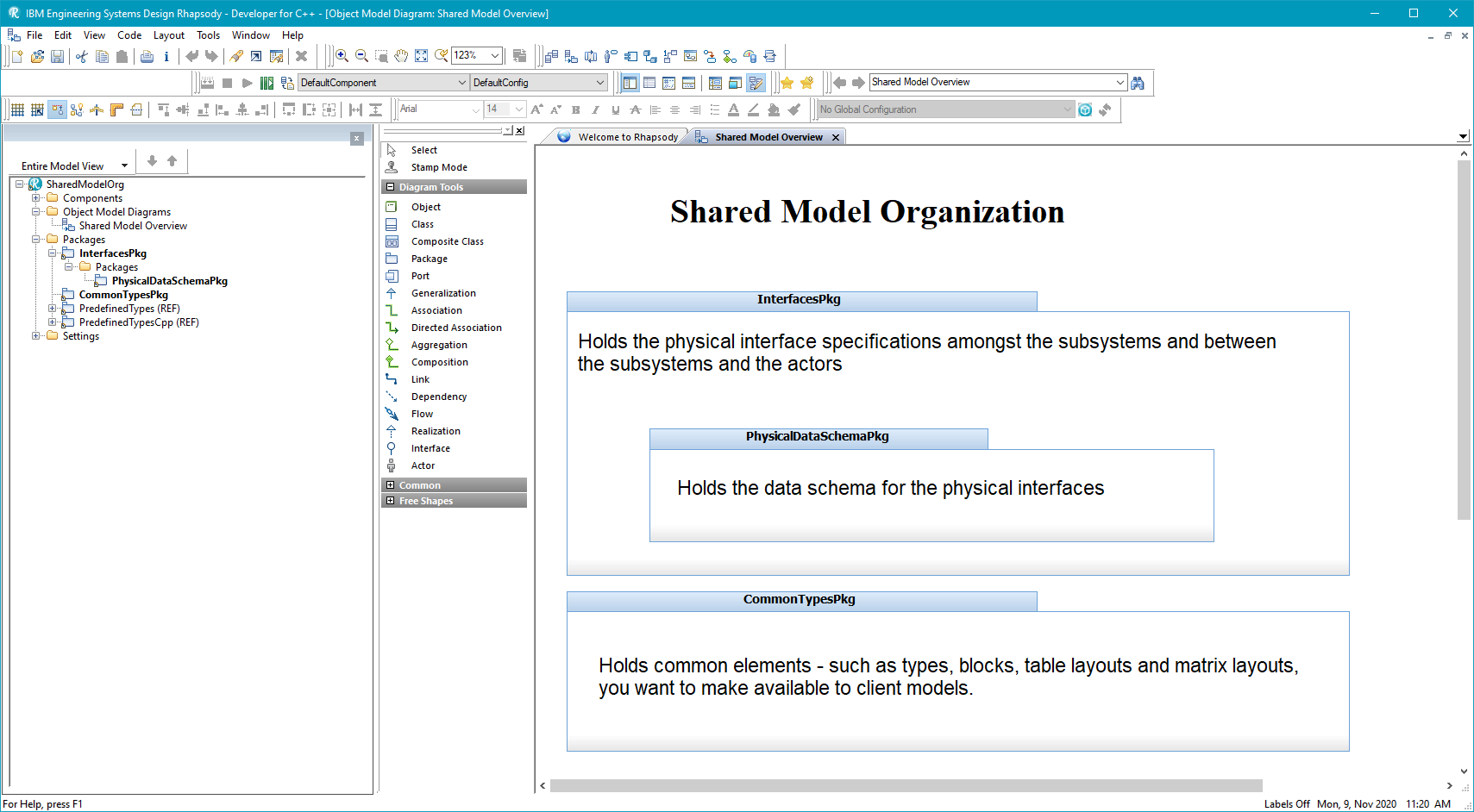


Figure 4: Shared Model Organization

## Naming Conventions

### Basic Naming convention

Figure 5 through Figure 8 show examples of the following naming conventions:

* Model element names shall be taken from the appropriate domain vocabulary, whether it is a problem-domain (e.g. Tracking or Navigation) or technical design (e.g. middleware or hardware) domain
  + In general, no “default names” assigned by the tool are acceptable in a model under formal review or considered to be final
  + Exceptions: There are some exceptions where the name is almost never used, such as the name of the state machine for a block; it is almost always referenced as being owned by the block and so the default name is acceptable.
* Model element names shall not contain white space or “special characters” except for the underscore (“\_”).
  + In general, names must be “compilable”. This is necessary to support executable models.
* Blocks, interface blocks, and data types begin with an uppercase letter
* Event names begin with a lowercase letter, as in “evKnobTurn”
* Block property names will begin with a lowercase letter. Block features include
  + Block value properties
  + Block functions (operations)
  + Block event receptions
  + Block ports
  + Block association roles
  + Block parts
* Block instance (part) name will begin with a lowercase letter.
* “Things” (e.g. objects, blocks, value properties) shall be named with strong nouns or noun phrases
* Packages names will begin with an uppercase letter, have a name that is consistent with its purpose, and end with “Pkg” as a suffix. For example, “DesignPkg” or “UseCasePkg”.
* “Actions” (e.g. operations, use cases, functions) shall be named with strong verb or verb phrases
* Association role names shall refer to the usage or role an instance of the block plays with respect to the block at the other end of the association, e.g.
  + myDataSource
  + itsDataQueue
  + theCommController
* In multiple word names, make the first letter of every word (after the first) upper case. This is known as *camel case* as in ThisIsABlock (for a block) or thisIsAProperty (for a property).
  + Underscores may be inserted between words, if desired as in This\_Is\_A\_Block (for a block) or this\_Is\_A\_Property (for a property).
* Port names shall begin with a lower case “p” and be named either by
  + Their semantic content (e.g. pConfigData)
  + The element to which they connect (e.g. pTracker) (preferred)
* Interface blocks shall be named either
  + in terms of their semantic concept (e.g. iNavData or iFLIRCommands) and their names shall be prefixed with a lower case ‘i’ OR
  + by the name of the contributing elements (e.g. iSource\_Target, where “Source” refers to the unconjugated side of the interface and “Target” refers to the conjugated side) – see the iTrackFuser\_TargetManger interface block in Figure 5. (preferred)
* Named constants shall be named with ALL CAPS, as in MAX\_FLOW\_RATE.

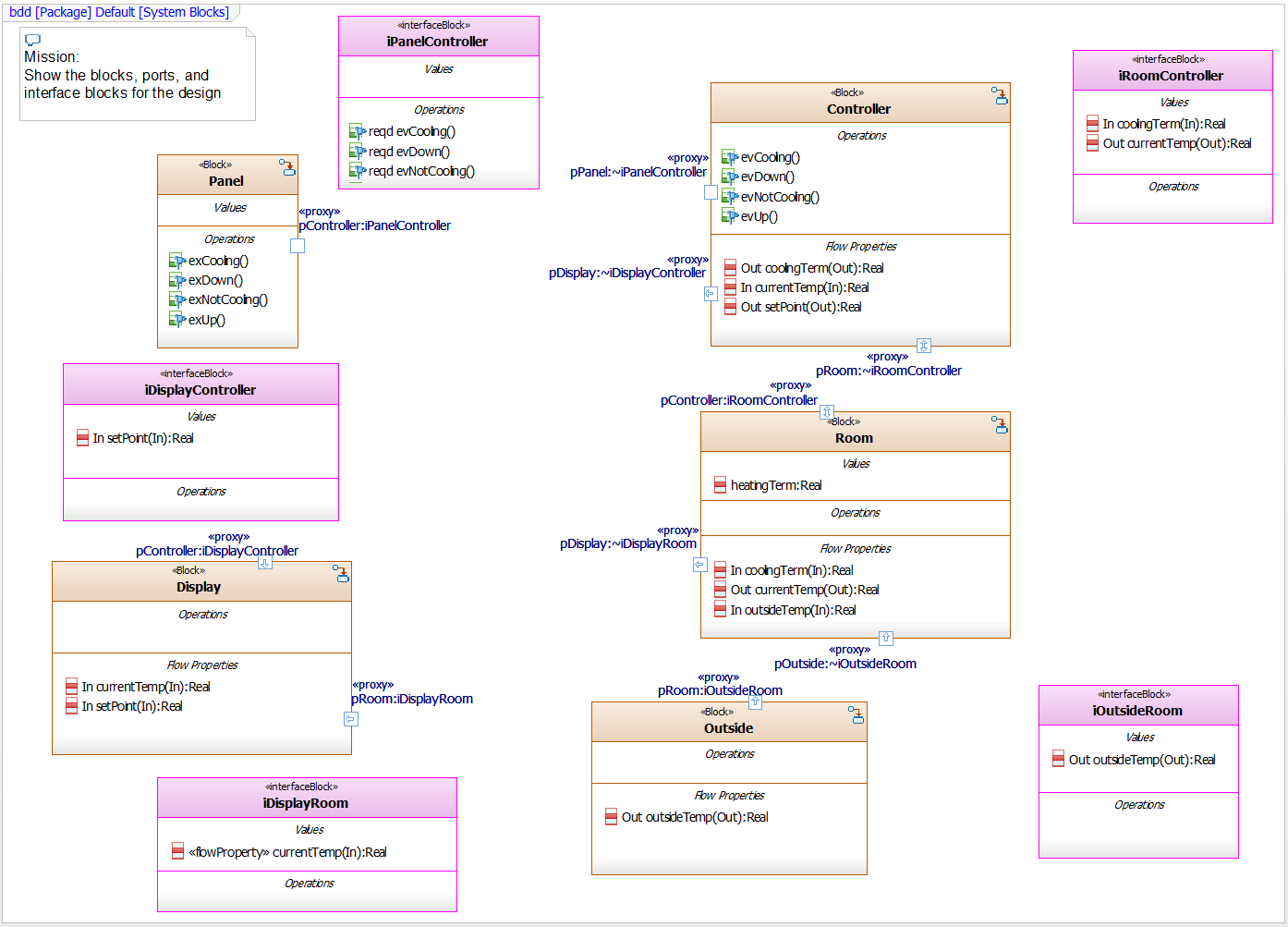


Figure 5: Naming Blocks and Features on a BDD

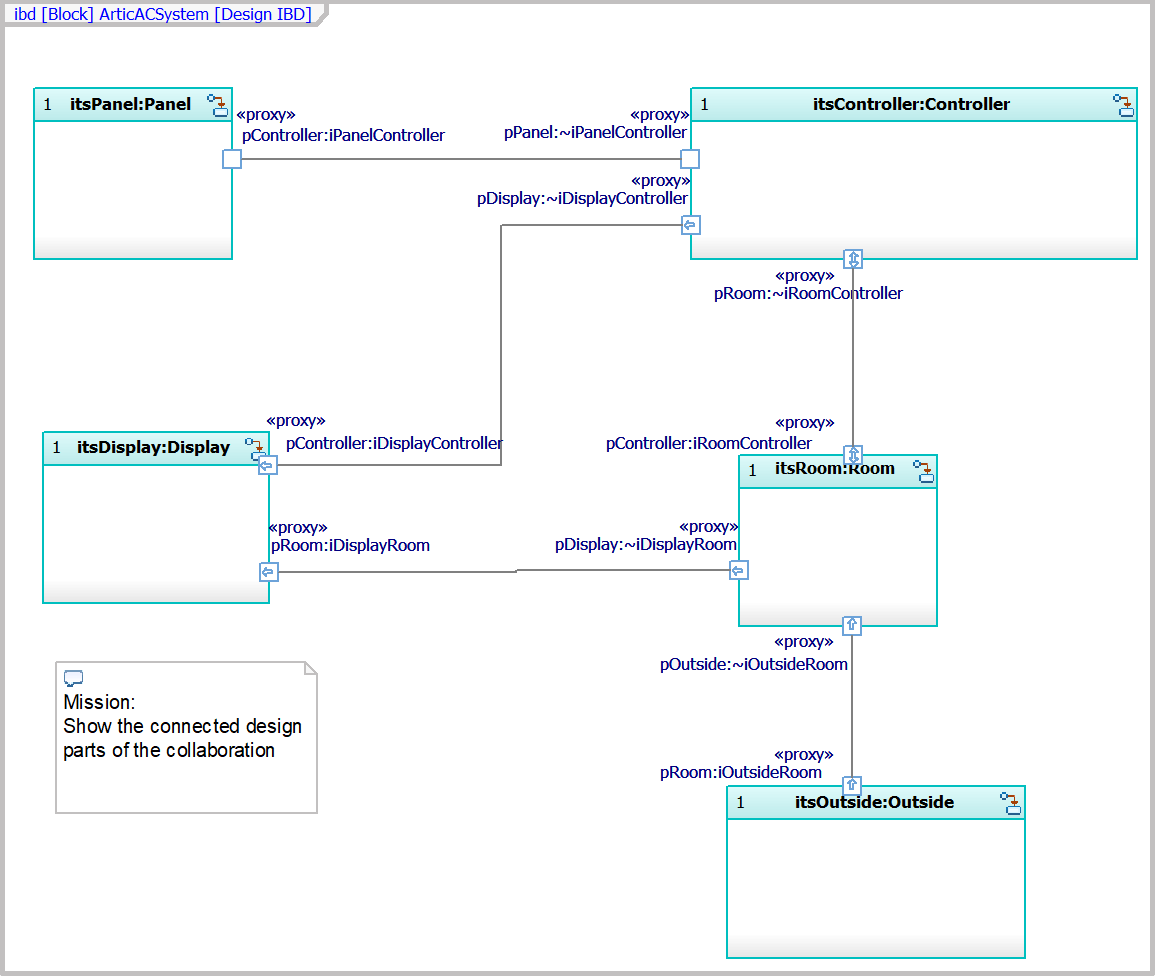


Figure 6: Naming on an Internal Block Diagram

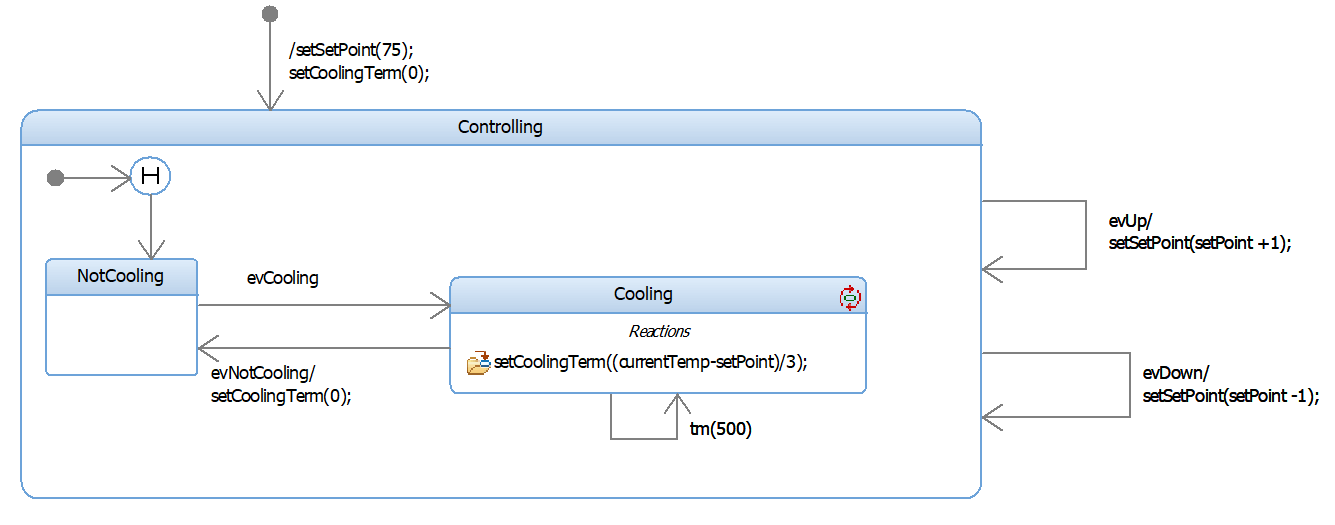


Figure 7: Naming States and Transitions

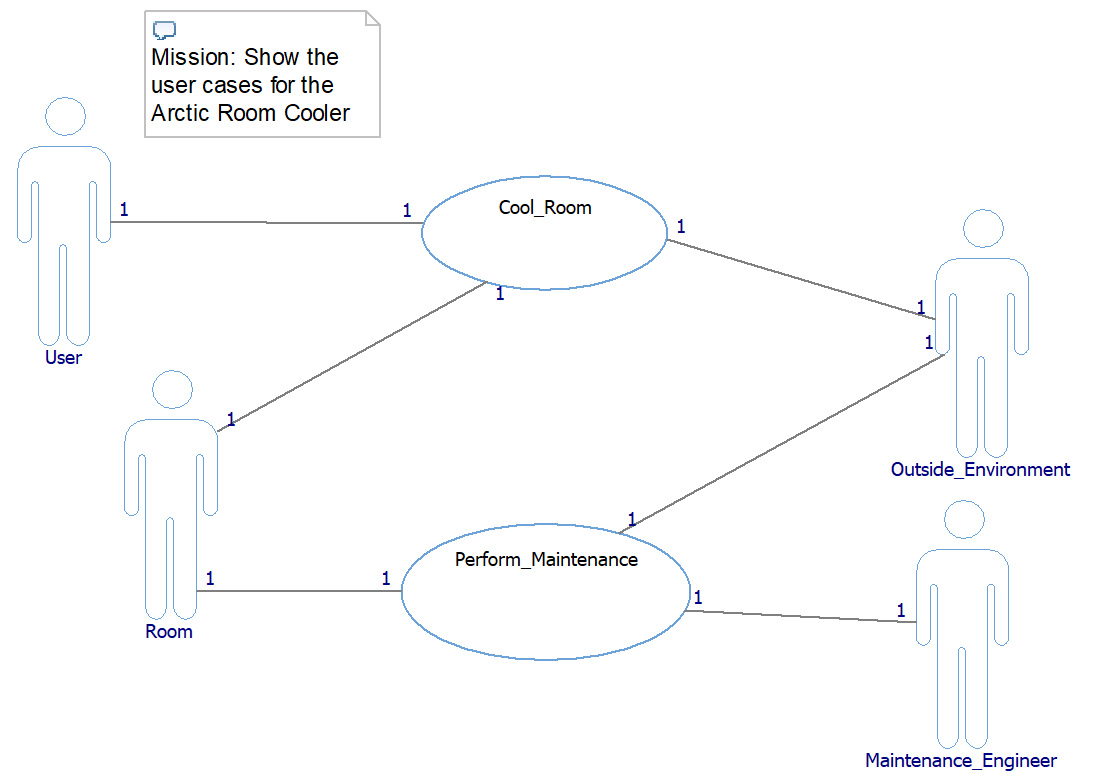


Figure 8: Naming Use Cases

## General Diagramming Conventions

### Every diagram shall have a singular mission

Every diagram shall have a single important concept that it is trying to show as shown in Figure 9. This is called its *mission*. This is especially important for block, activity, parametric, and sequence diagrams (less important for state diagrams due to their “built-in” mission).

A diagram shall show elements related to a single purpose – a singular concept, a question (or answer), or to support a line of reasoning. This is the *mission* of the diagram.

The mission shall be stated on the diagram. Some common block diagram missions include

* Show a use case execution context
* Show a design-level collaboration
* Show a single generalization taxonomy
* Show a logical or physical data schema
* Show the contents of a package
* Show an aspect of system architecture
  + Show the subsystem architecture
  + Show the concurrency architecture
  + Show the distribution architecture
  + Show the deployment architecture
  + Show the safety architecture
  + Show the reliability architecture
  + Show the security architecture
* Show a design pattern

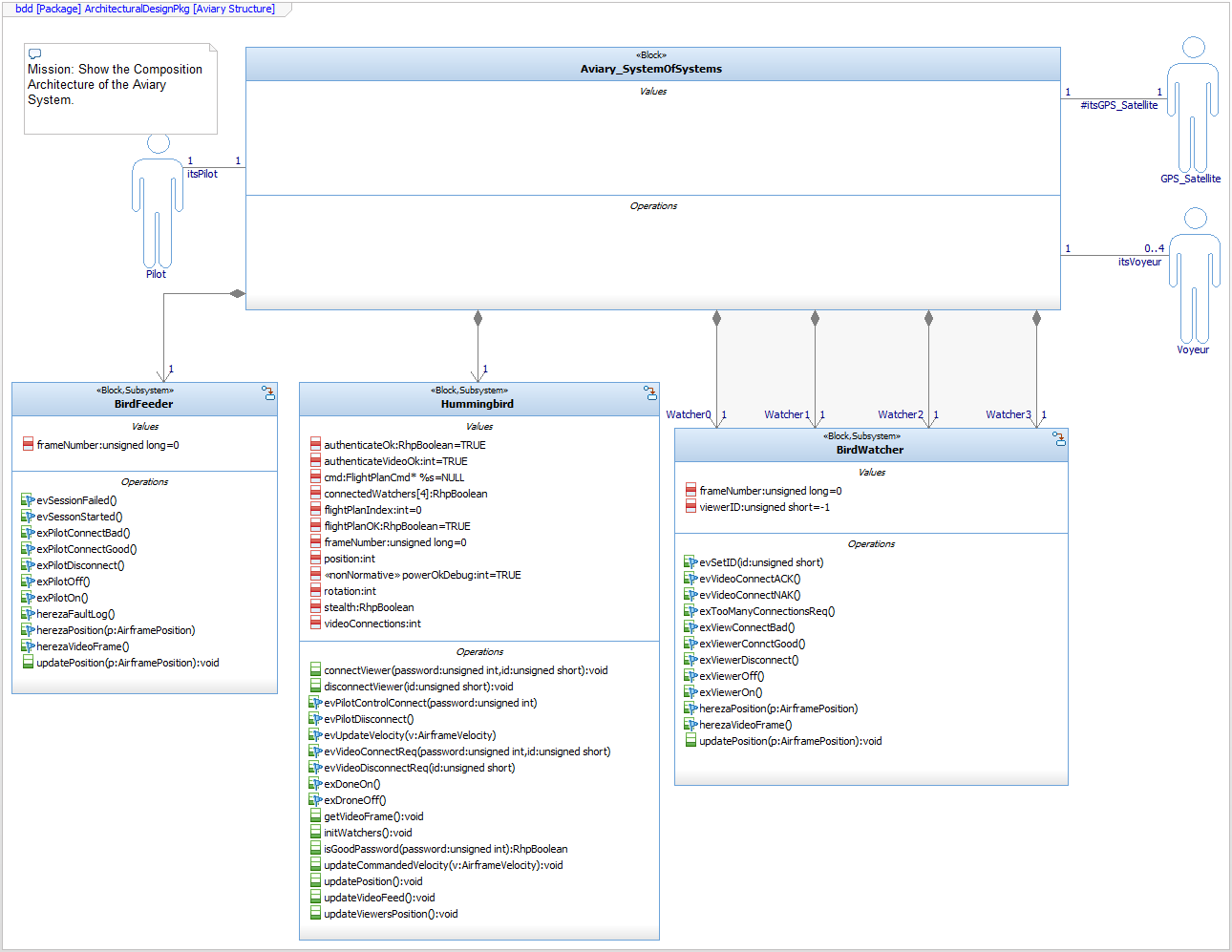


Figure 9: Example Block Diagram with Mission

* Very complex diagrams usually have too many missions or only a vague purpose

### Other diagramming conventions

* Every structural (BDD or IBD), requirement, package, sequence, use case, activity diagram, and parametric diagram shall have a comment explicitly describing the mission or purpose of that diagram
* Structural diagrams include
  + Block Definition Diagram (BDD)
  + Internal Block Diagram (IBD)
* Every interaction diagram shall have a shall have a comment explicitly describing
  + The corresponding use case (if applicable)
  + The mission or purpose of that diagram
  + The pre- and post-conditions of the diagram
* Interaction diagrams include
  + Sequence diagram
  + Timing diagram (UML)
* Functional diagrams include:
  + Use case diagrams
  + Requirements diagrams
* Minimize line crossing. To avoid line crossing:
  + Use diagram connectors. These are elements for showing line connections when it is inconvenient to draw the line between the two elements
  + Replicate a block or diagram element. It is perfectly permissible to show a block or type multiple times on a diagram. Do this when it minimizes diagrammatic complexity.
  + Use multiple diagrams
* As much as possible, inputs shall come from the left or top and output shall leave at the right or bottom
* Use similar line styles (straight, rectilinear or curved) for semantically similar lines (e.g. rounded rectilinear for associations control and object flows, and state transitions, straight for generalization and dependencies).
* Avoiding using color to show semantics
  + Color may be used for emphasis or to improve readability
* Add constraints to show special or custom semantics or user-defined semantic rules
* Create a Model Overview Diagram (usage of Package Diagram or BDD and stereotyped with «Model Overview Diagram» from the Safety Profile) as a project-level diagram (i.e. not nested within a package) that contains
  + Model organization description
  + Package structure shown as packages
  + Provide hyperlinks on the model overview diagram to important model views such as
    - High-level use cases
    - Type Context
    - Connected Context
    - Composition Architecture
    - Connected Architecture
    - Trade study and other parametrics of interest

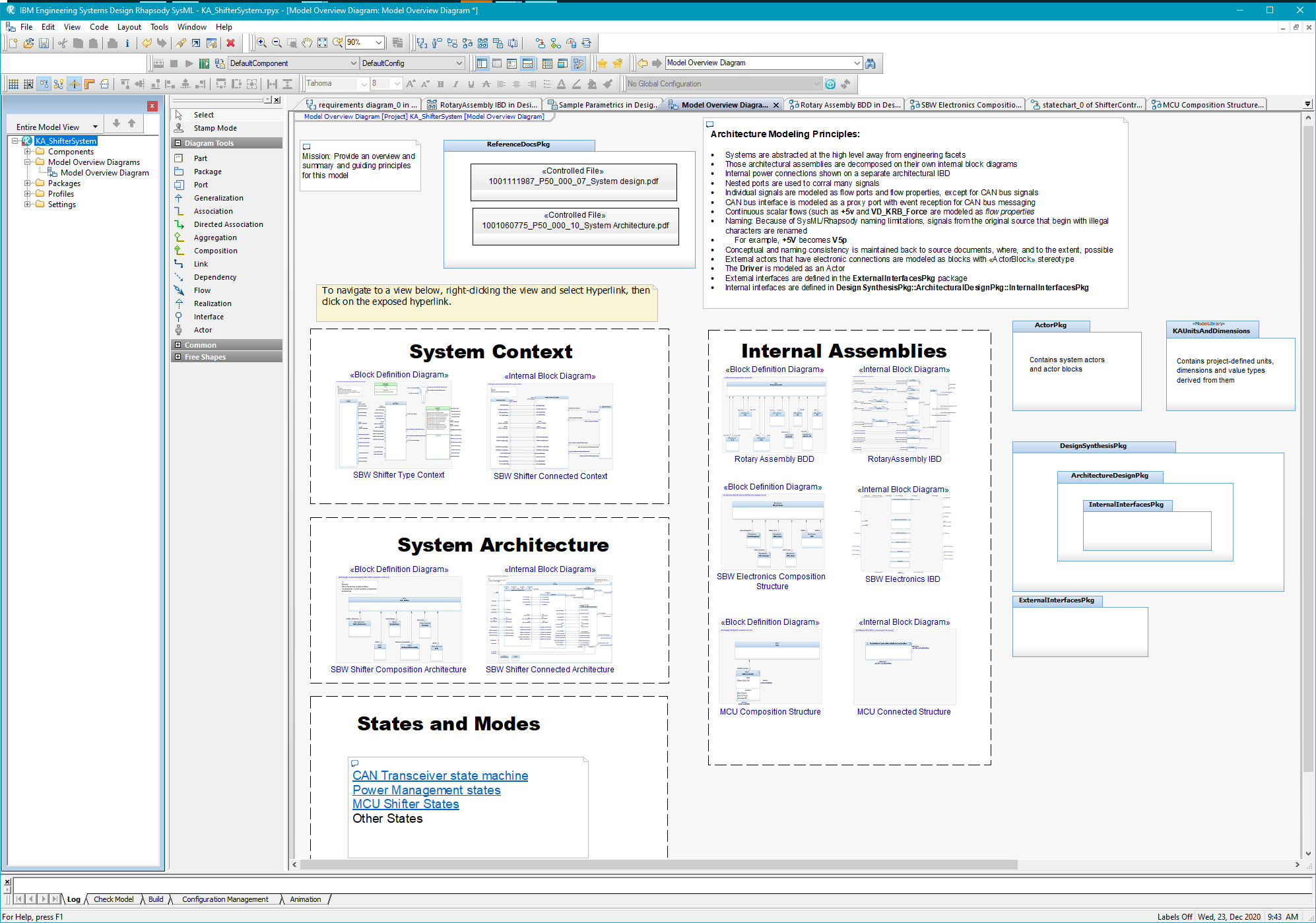


Figure 10: Example Project Overview diagram

## Block Definition Diagrams (BDDs)

### Content

BDDs are generally limited to

* Blocks
* Types, Dimensions, and Units
* Block properties
  + Value Properties
  + Operations
  + Event Receptions
  + Ports
  + Nested parts (instances)
* Constraint blocks
* Interface blocks
* Block relations:
  + Association, Aggregation, Composition
  + Generalization
  + Dependency (including stereotypes of dependency)
* Comments
* Constraints
* Requirements

In Rhapsody, BDDs may also contain parts and connectors and may be used instead of IBDs, if desired.

### Block and Parts

* Blocks, parts, and attributes shall have names that are noun or noun phrases.
* Blocks, parts, and attributes shall have *singular* nouns for names
  + Plurality is handled with multiplicity of the element or role end of the relation
* Operations shall be named with a strong verbs or verb phrases
* Only show block features if they contribute to the diagram mission.
* Value properties and operations shall have *protected* visibility unless their access is directly required by client blocks

### Interfaces

Interfaces shall only be used when ports are not used and it is desirable to show interface; otherwise proxy ports and interface blocks shall be used.

* Note: Interfaces may be used freely in UML software models, as needed.

### Interface Blocks and Ports

* If ports are used, only *proxy and flow ports* are allowed; avoid *full and standard (UML) ports* in system models.
  + Note: standard UML ports may be used in UML software models, as needed.
  + Note: standard UML ports may be used if they are expected to be used directly in UML software models derived from this model
* Flow ports shall only be used with the Simulink Profile to interface Rhapsody and Simulink models.
* Proxy ports are typed by Interface Blocks.
* Ports shall be named in terms of the client role that connects to it or the semantic content of the data or services that traverse it, as shown in Figure 11.



Figure 11: Interfaces and Ports Example

* Interface blocks shall not define or reveal design or implementation of the block realizing the interface.
* Interface blocks shall not contain value properties
* Interface blocks may contain flow properties
* Services within blocks (operations or event receptions) shall be stereotyped as «directed features» and their direction – *required* or *provided* – must be specified
* Service flow direction *providedrequired* shall be avoided.

### Relations

* The use of ports is an *alternative* to the use of associations:
  + Ports can only be connected between instance or instance roles but they are specified on blocks.
  + Associations are relations between blocks; links (connectors) are instances of associations
* Always show multiplicity on associations
  + Exception: you need not show the multiplicity on the “whole” end of a composition, as this is always “1”
  + Exception: you need not show the multiplicity on the owner end of a directed association
* Use role ends names on associations
  + Show responsibilities via good role end naming
  + Role end names shall specify a usage that one or more instances at that role end fulfill at run-time
  + Role end names are always more important that association names
* Always show role names on associations
  + When there are multiple associations between a pair of classes
  + Exception: only show role end names for navigable ends of the association; that is, for a directed association, only show the role end of the navigable end (the end with the arrow).
* Use a single association with non-unary multiplicity when all the objects play the same role; use multiple associations to the same class when the objects play different roles
  + Figure 12 shows two different compositions to MessageQueue because the roles of the two are distinct (one is for input, the other for output)
  + The figure shows a \* multiplicity for Message, because each message fulfills the same role with respect to the MessageQueue



Figure 12: Relations Example

* Role end names (see Figure 12) shall indicate the role that an instance of one block plays for the other, e.g.
* Most associations should be unidirectional
  + Most associations model a client-server relation with the client being able to navigate to the server, but not vice versa.
  + Early models may use bidirectional associations when the direction of message flow isn’t clear but later models should resolve most of these into unidirectional associations
* Use rectilinear lines for association (including aggregation and composition) and straight lines for generalization and dependency
* Minimize use of dependency relation
  + For requirements traceability, use the «trace» dependency (if done in the model rather than in a separate requirements traceability tool)

## Internal Block Diagrams (IBDs)

IBDs are used to show how instances (parts) connect via *connectors*, with or without ports.

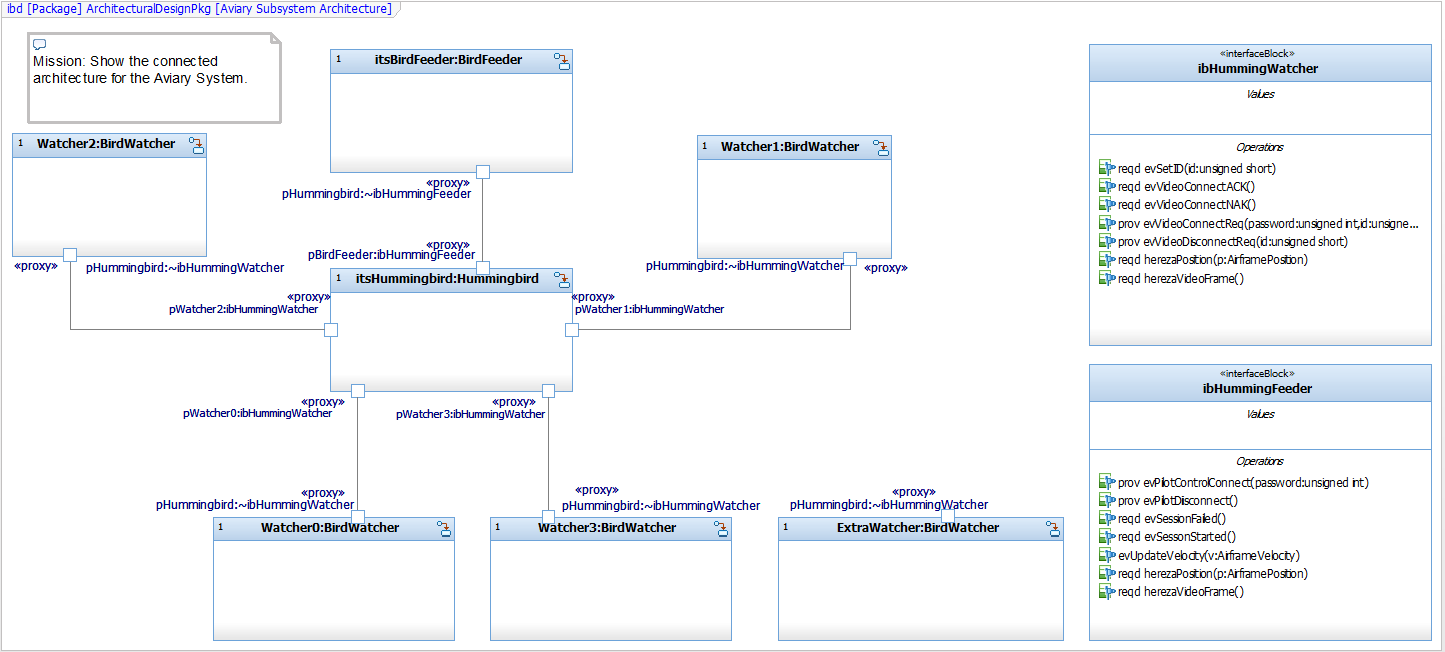


Figure 13: Example IBD

* IBDs are generally owned by a composite block but may be owned by a package
* Ports are linked via *connectors*
* Connected ports must be interface block-compatible (conjugated and unconjugated applications of the same interface block)

## Use Case Diagrams

### Use Cases

* Adhere to general diagram guidelines, above
* Model an operational capability as a use case
* For each use case, specify in the description (see Figure 14)
  + Use case name
  + Purpose or goal
  + Description
  + Preconditions – invariants that must be true before the use case is started
  + Post-conditions – invariants the system guarantees when the use case completes
  + Invariants – assumptions or expectations that must be true throughout the execution of the use case behavior

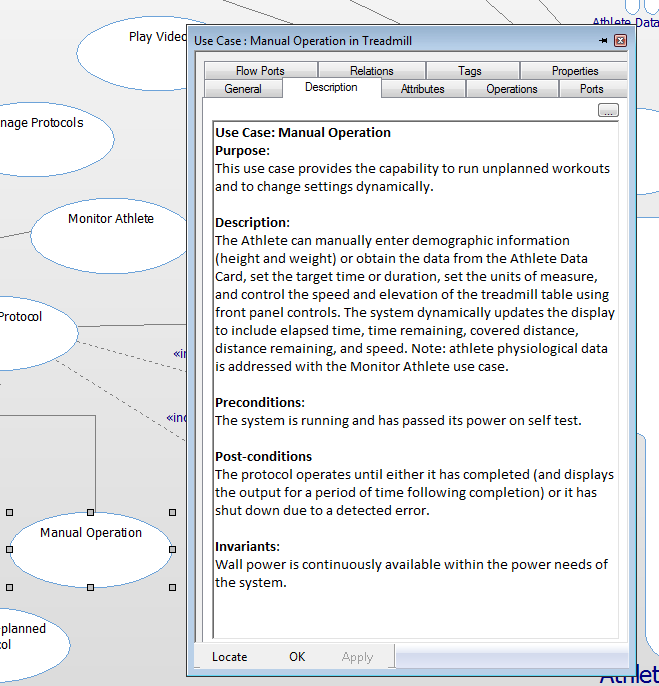


Figure 14: Use Case Description

* Use cases shall be named with a strong verb or verb phrase
* Use cases shall be independent in terms of the requirements as much as reasonable (but needn’t be in terms of their design realization)
  + Example: “Configure Sensor” and “Acquire Data” are independent in terms of their requirements, but in the implementation, the configuration settings are used in the acquisition of the data
* If use cases are tightly coupled in terms of operational requirements, join them into a single use case
  + E.g., “Manage Pedestrian Traffic” and “Manage Vehicular Traffic” are tightly coupled; join these into a “Manage Traffic” use case
* Constrain a use case only when that constraint applies to all scenarios of the use case
* All use cases shall interact at least one actor
* Define a use case with both scenarios (sequence diagrams) and specifications (activity and/or state diagrams)
* Use packages and/or use case diagrams to manage many use cases, organized by some criterion, such as
  + Common actors
  + Common purpose
  + Common area of concern
  + Common specification team

### Actors

* Actors are objects outside the scope of the system that interact with the system when it executes the use case
* Actors shall be given singular noun names from the problem domain
* If it’s “in the box” released from manufacturing, then it’s not an actor
  + If it connects to or interacts with your system at the customer site, then it is an actor
* Avoid identifying technology as actors; the actors should be the problem domain element of interest, not the means by which the actor connects to your system
  + The actor might be “Hospital Information System” not the “Network Interface Card” that connects the HIS to your system
* Don’t model interaction among actors
  + Since you’re not building the actor, their interaction is unimportant in your system design – focus on what you’re trying to build
* NEVER model “Time” as an actor; a use case can initiate behavior on its own with internal timeout events

### Relations

* Use directed associations when message flow is unidirectional
* Subclass actors when the specialized actor participates in special relations or additional use cases over the base actor
* Use generalization to indicate specialized forms when technology realizations add distinct requirements
  + E.g. “Identify User” use case holds requirements common to all its specialized forms, but “Identify via Fingerprint Scan” adds some unique requirements over “Identify via Password”
* Use «include» to map system-level use cases to subsystem-level use cases
* Use «include» to encapsulate capabilities that are used in multiple (larger) use cases
* «include» arrowhead shall point to the “part” use case, not the “whole”
* Use «extend» infrequently
* Use «extend» for optional functionality that can be inserted at a specific extension point
* «extend» arrowhead points toward the “whole” use case, not the “part”
* Use «trace» to show the relation between a use case and a requirement allocated to it

## Requirements Diagrams

Requirements will be managed primarily in DOORS. The use of requirements diagrams and relations are limited to adding relations from model element to requirements. Requirements diagrams and tables may be used to visualize requirements in the model, if desired.

### Relations

* Dependency relations «trace», «satisfy», «allocate») go FROM the source element (use case, block, or other design element) TO the requirement
* Use «trace» for use case – requirement relation
* Use «satisfy» or «allocate» for design element – requirement relation

## Requirements Tables

Requirements tables may be used to visualize sets of requirements in Rhapsody.

The SysML profile provides a predefined requirements table. An example of its use is shown in Figure 15.

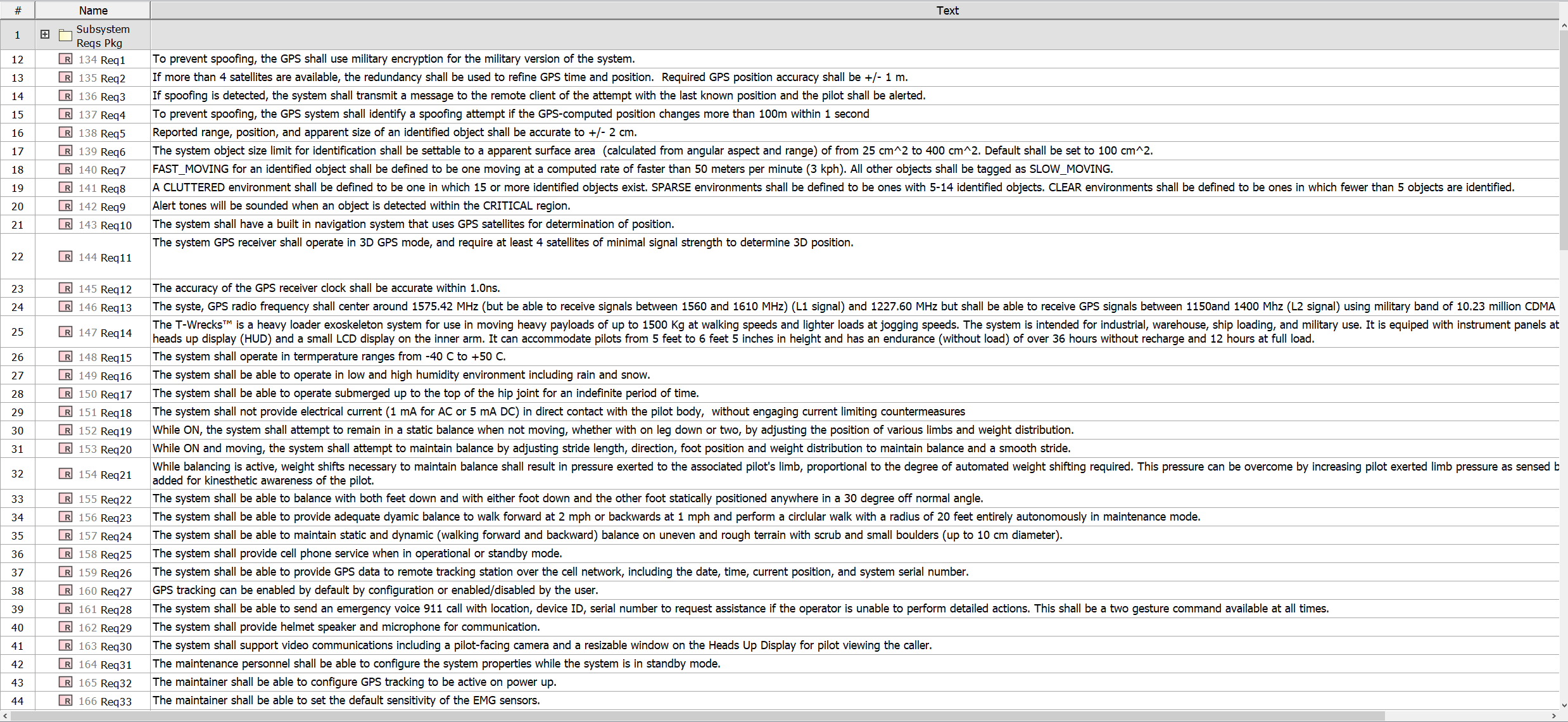


Figure 15: Requirements Table

## Matrices

Matrices show the relations between sets of elements. Common uses for matrices include:

* Stakeholder – System Requirements
* Requirements – Use Cases
* Requirements – Design Elements

Some matrix layouts are provided in the Harmony SE Profile that ships with Rhapsody, and others by the Safety Profile. Other matrix can be easily developed as needed.

## Sequence Diagrams

* For a set of sequence diagrams around a common context – such as a use case or design collaboration – it is preferrable to have the lifelines appear in the same order, even if a lifeline is not used in a particular sequence diagram. This is to facilitate comparison among the sequences.
* As much as possible, arrange the lifelines to make messages go from left to right.
* Use horizontal lines for synchronous messages
* Use either horizontal or slanted lines for asynchronous messages
* Execution occurrences (“activation bars”) on lifelines shall be avoided.
* Add comments to the sequence to describe why steps are being taken and to describe parallel activities not shown in the messages
* To shorten long scenario, wrap up sets of related messages into a referenced interaction fragment, as shown in Figure 16.

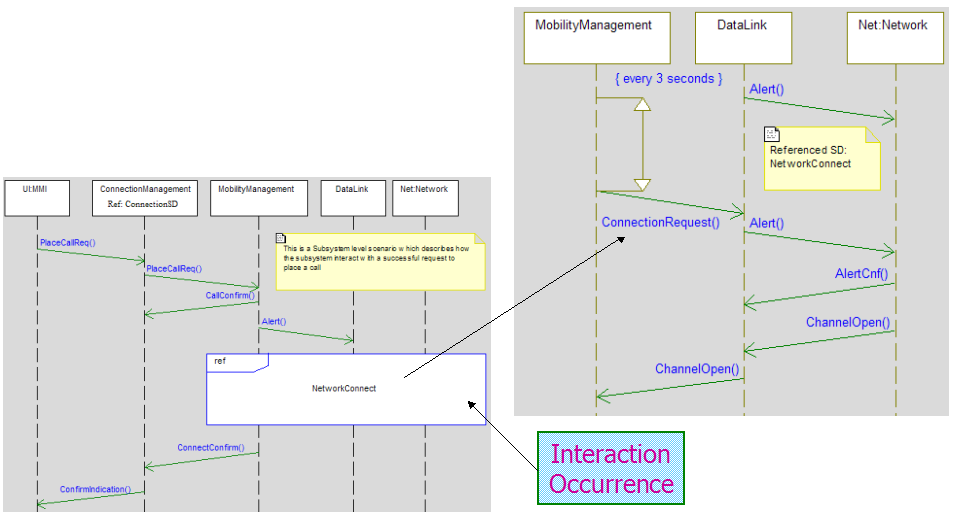


Figure 16: Interaction Fragment

* To reuse sets of messages, use a referenced interaction fragment
* Name messages the same as the operations or events they represent or invoke
* For special semantics use relevant interaction fragment operators, e.g.
  + Loop
  + Parallel
  + Opt (optional) for “if”
  + Alt (alternative) for “select case”

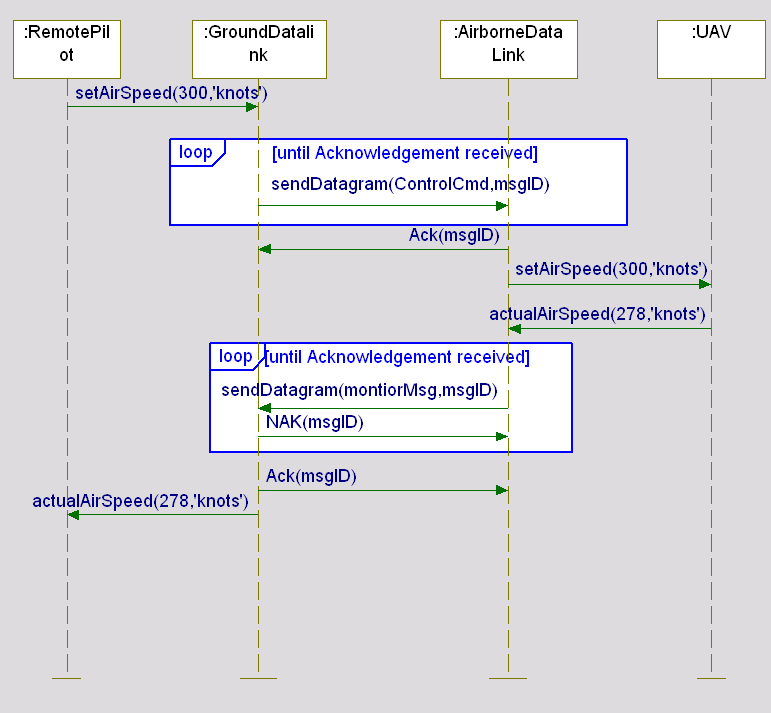


Figure 17: Loop Operator

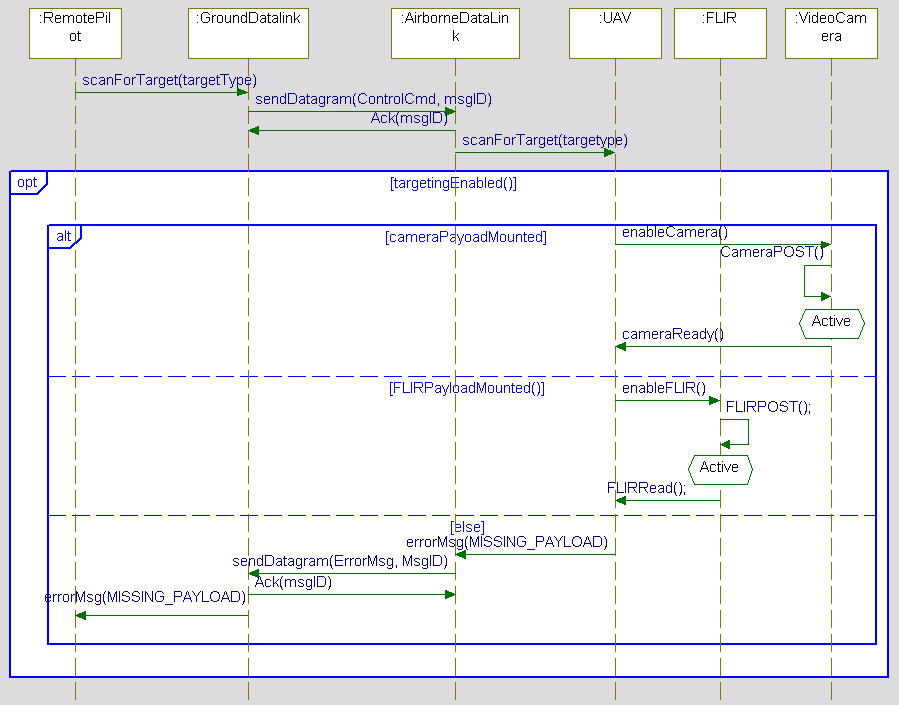


Figure 18: Opt and Alt Operators

* Avoid nesting interaction operations more than three levels deep.

## Activity Diagrams

* Use activity diagrams to model behavior that is primarily flow (rather than event-) based such as algorithms or when modeling behavior that is continuous in time or value such as continuous pressure on a pedal
* Model algorithmic behavior (flow of control) with activity diagrams
  + Flow of control in operations can be specified with activity diagrams
* Always indicate starting action in an activity diagram
* Primitive actions shall be specified in the target action language (C or C++)
* You may optionally use forks and joins to model “logical concurrency” in activity diagrams but note that this will not create task threads (use active classes for that, although that is not normally a systems concern).
* Optionally, swim lanes may be used to allocate activities to classifiers (such as blocks)
* Use guards only on control flows exiting a condition or branch point
* Complexity in activity diagrams is managed by decomposition
  + Use *Call Behavior* actions to invoke behavior on a separate activity diagram
  + Use *Call Operation* actions to invoke behavior defined by a function or operation
* Activity diagrams and state machine should generally be mixed with the statechart “on top” and the activity diagrams specifying behaviors of actions on that state machine

## State Diagrams

* State diagrams should be used preferentially to specify reactive (i.e. “reacts to events”) behavior for actors, blocks and use cases, including blocks at different levels of abstraction (e.g. systems and subsystems)
* Use a statechart to model behavior of classifiers when that behavior
  + is event driven or
  + is modal, i.e. the behavior differs depending on state
* Always, at every level of nesting, indicate the default state unless there is only one state at that level of abstraction
* State diagrams may be either asynchronous (asynchronous event-driven) or synchronous (call-driven)
  + Do not mix synchronous and asynchronous event triggers in the same state machine
  + Great care must be taken with state machines with both synchronous and asynchronous triggers to avoid race conditions

### States

* Use names for states that come from the problem vocabulary (domain)
  + Exception: In some cases, a state may be added to explicit force the completion of a run-to-completion step using the [*Forced Closure Rule*](#_Definitions_and_Acronyms). Such states will have names outside of the problem domain because they exist solely to resolve a design technical issue.
* Use composite states when one transition exiting the composite applies to all nested states or when the composite state logically contains the nested states (e.g. note the evEOS event from ParsingNumber state in Figure 19).



Figure 19: Nested States

* Use submachines to simplify complex state machines such as shown in the following sets of figures. Figure 20 shows a complex statechart with 3 levels of abstraction before it is decomposed into nested submachines. Figure 21 through Figure 23 show exactly the same statechart decomposed into a set of layered submachines.



Figure 20: Complex statechart before decomposition into submachines

This complex state machine contains a composite state Parsing Expression, which in turn contains a composite state Parsing Term. This can be decomposed into three layers:



Figure 21: Statechart decomposed into submachines – level 0



Figure 22: Statechart decomposed into submachines – level 1



Figure 23: Statechart decomposed into submachines – level 2

* Pay attention to action placement
  + Add actions to state entry only when the actions should be executed whenever the state is entered regardless of which transition is taken
  + Add actions to state exit only when the actions should be executed whenever the state is exited regardless of which transition is taken
  + Add actions to transitions when the above conditions are not met
* In the presence of and-states, avoid race conditions
  + Race conditions are defined to be when a computational result depends on a specific order of execution, but that order is not knowable
  + Race conditions occur when the same event is processed in simultaneously active and-states and
    - Incompatible target states are specified, or
    - Actions on the transitions manipulate the same attributes, or
    - Incompatible actions are executed
  + See Figure 24 for an example of an avoidable race condition

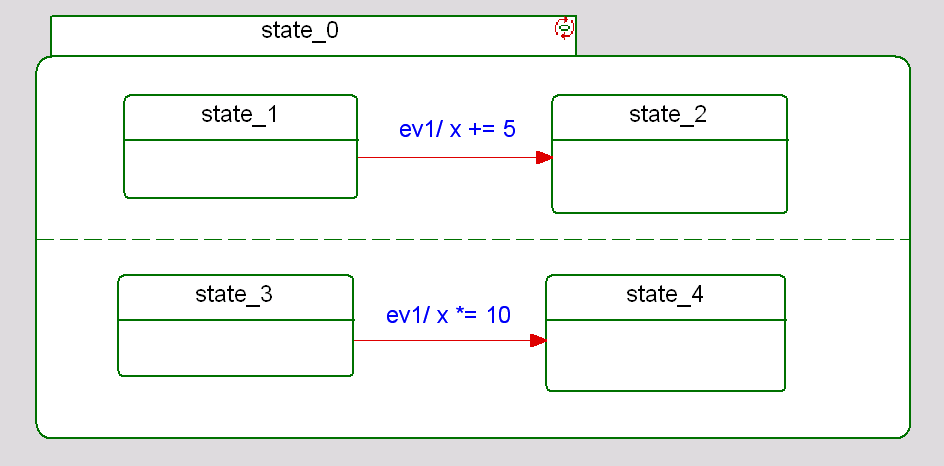


Figure 24: Race Condition in And-States

### Actions

* Actions are run-to-completion, therefore actions should generally have a short execution time
* Actions may be direct attribute manipulations, operations defined on the class, or operations defined on classes to which the current class has an association
* Primitive actions shall be specified in the model’s action language (C or C++)
* Complex actions shall be modeled as operations; those operations can then be specified using activity diagrams
  + E.g rather than “/x = foo(z); y = sin(x)^2 – tan(x); z = sin(x + y);”, wrap the set of actions in to an operation and invoke it “/computeZ();”
* Simple actions may be direct action language statements to manipulate attributes of the object
  + E.g. ev1/ x = sin(y) + cos(z);

### Guards

* Guards shall not have side-effects
  + In C, C++, or Java, “x = 0” shall not be used as a guard as it performs an assignment; “x == 0” is preferred
* Guards on transition segments exiting conditional connectors shall have non-overlapping conditions
  + For example, “[x>0]” and “[x>10]” would not be good guards from the same conditional connector; if x==20, then both guards would evaluate to TRUE
* Don’t use the result of actions in guards on the same transition
  + Guards are evaluated prior to the execution of actions
  + See [*Forced Closure Rule*](#_States) above
* Use an [else] guard when the event triggering the transition must always be handled

### Submachines

A *submachine* is a set of nested states that are placed in a separate diagram to decrease the visual complexity of a state machine.

* Remember that submachines are “syntactic sugar” only – the submachine is still logically a part of the containing state machine; submachine merely aid in visualization of complex state machines
* Use submachines to manage complexity
  + when a composite state is part of a complex state machine, that composite state can be decomposed on a separate state diagram (submachine)
  + recommended when there are few, if any, non-default transitions
* Use exit and entry points only when non-default transitions are used
  + If there are more than a very small number of non-default transitions, it is recommended *not* to decompose the nested state into a submachine
* See State Guidelines and Figure 21 through Figure 23, above.

## Parametric Diagrams

Parametric diagrams are used to model the relation of parametric constraints and can be used to develop computation models.

* In Rhapsody, parametric diagrams may show Constraint Blocks as well as Constraint Properties.
* Constraint Parameters on Constraint Blocks shall be typed with an appropriate type.
* The directionality of Constraint Parameters on Constraint Blocks shall be specified.
* Constraints within Constraint blocks shall be well formed, according the syntax and semantics of the SysML.
* Parametric diagrams may be evaluated with the Rhapsody PCE Profile.

### Parametrics for architectural analysis

* The ArchitecturePkg::ArchitecturalAnalysisPkg is intended to hold analyses, including parametric analysis.
* It is expected that each different analysis will be in a separate subpackage nested within the ArchitecturePkg::ArchitecturalAnalysisPkg
* Trade studies are a kind of architectural analysis and are expected to be treated in this fashion.

# Semantic Standards: Using SysML

## Model Overview Diagram

* Each model shall have a Model Overview diagram located “above” the packages.
* This shall be either a Package or BDD diagram and the stereotype *«Model Overview Diagram»* from the *Safety Profile* shall be applied to the diagram
* This diagram shall contain information about the content and use of the model.

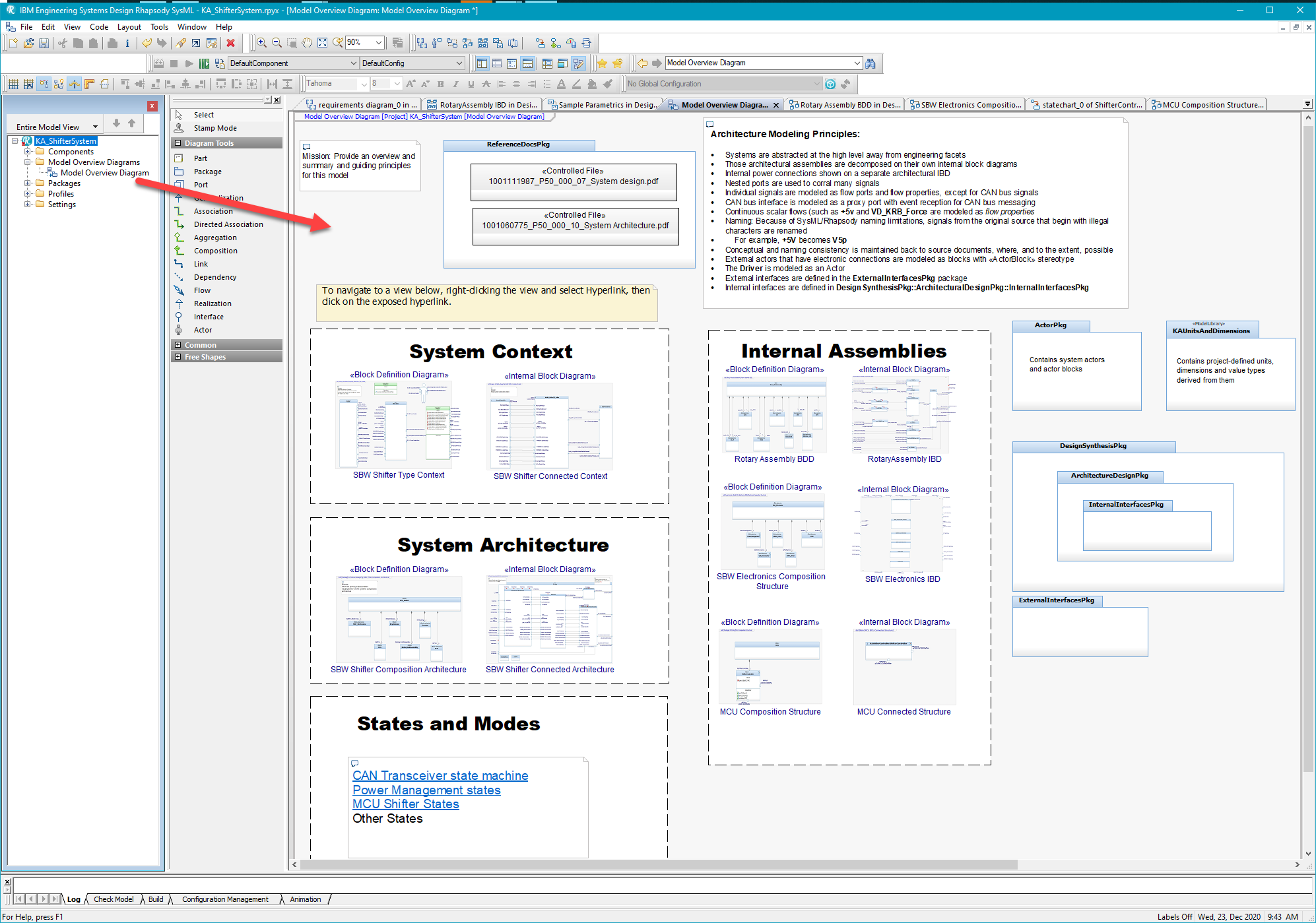


Figure 25: Model Overview Diagram

Note the location of the diagram in the browser on the left of Figure 25.



Figure 26: Another Model Overview Diagram

## Modeling Systems Architecture Context

* The system context shows the system as a block, the actors with which it communicates, and the interface blocks.
* Use BDD for the type context
* Use IBD for the connected context

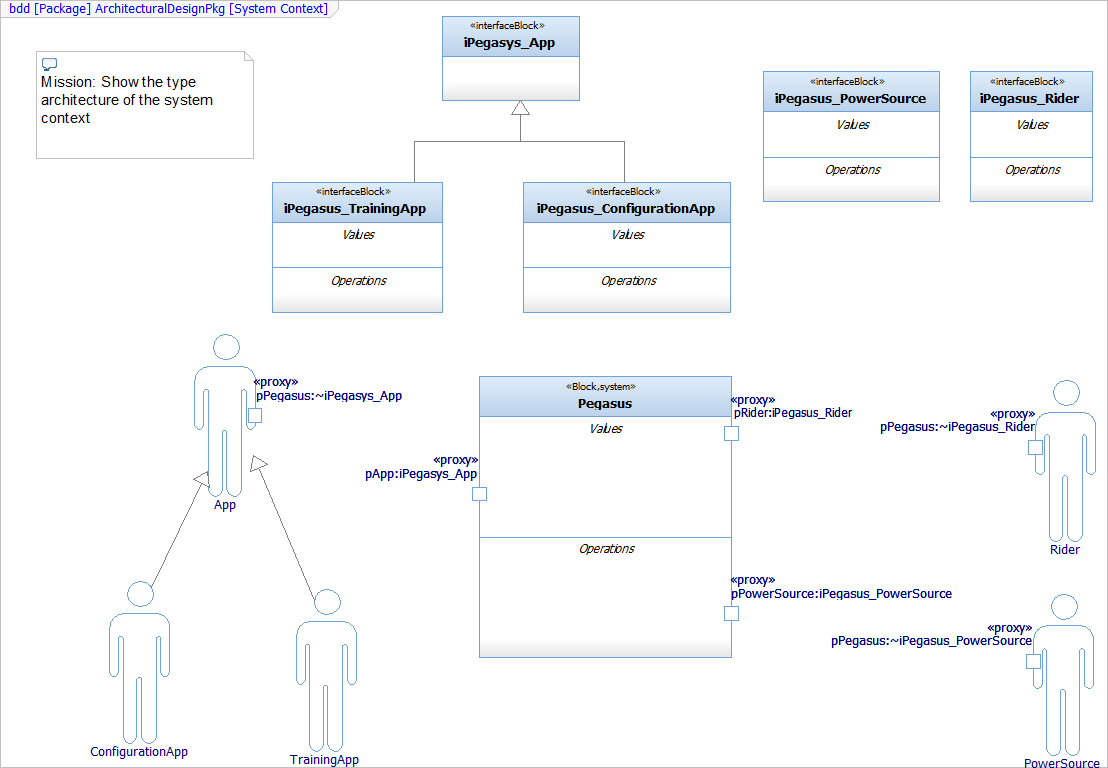


Figure 27: Type Context

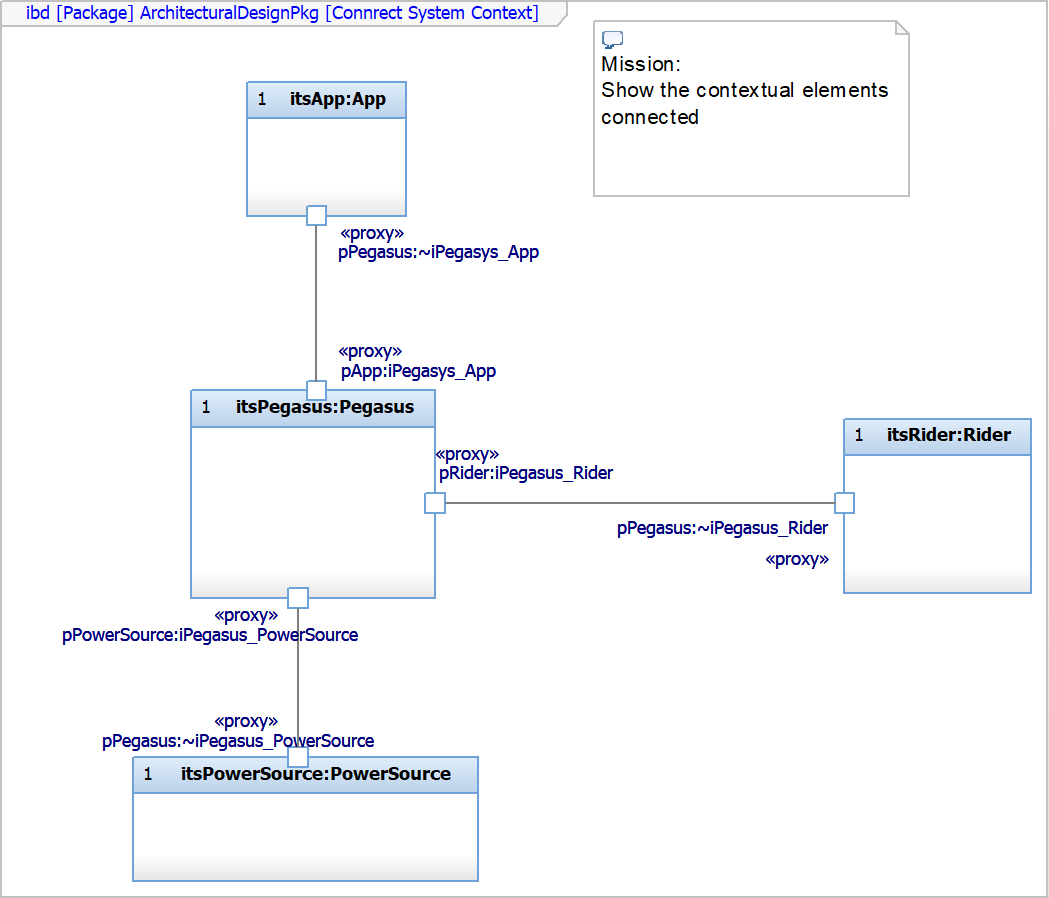


Figure 28: Connected Context

Modeling Systems Architecture Structure

* Use BDD to show the system composition architecture
  + The term “composition architecture” identifies the system and subsystems and show their relations.
* Use IBD to show the connected architecture
  + The connected architecture shows how the subsystems and related elements connect.

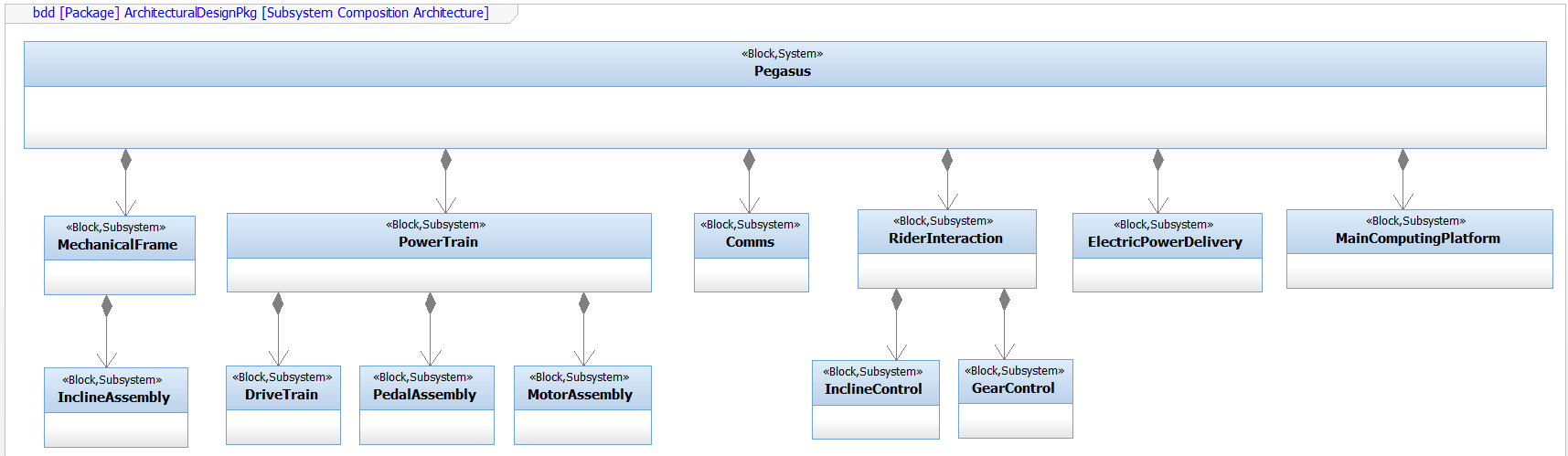


Figure 29: Composition Architecture

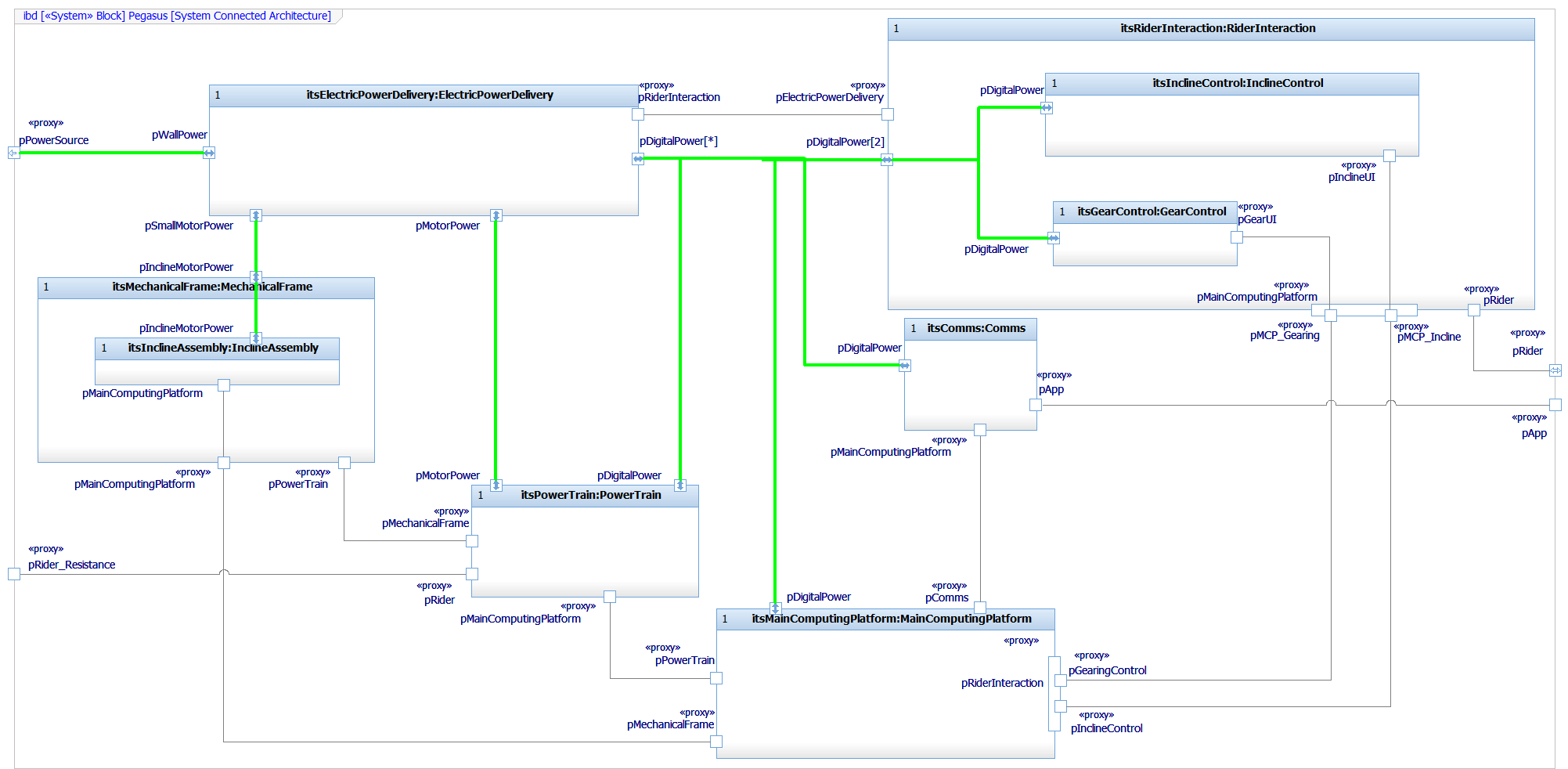


Figure 30: Connected Architecture

## Modeling Systems Architecture Behavior

Prefer state machines for behavioral specification of architectural elements. Interactions may be shown with sequence and/or activity diagrams, as desired.

### Modeling Data Schema

* Use BDDs to show the relations of blocks, types, dimensions, and units.
* Define and apply *units* preferentially over the use of primitive types
  + For example, define a unit KiloPascal and use it instead of just a double or Real.
* Use named constants rather than *magic numbers*
  + Define named constants as types in Rhapsody, with kind *Language,* and a definition using “#define”.

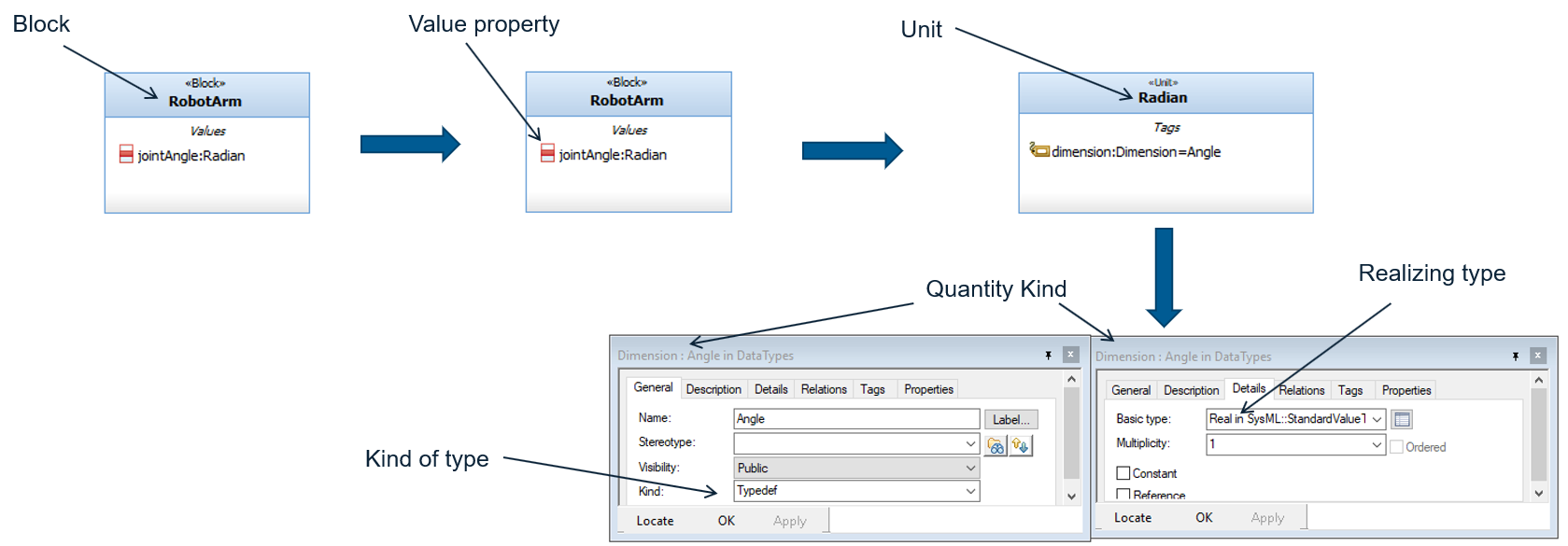


Figure 31: Type, Dimensions, and Units

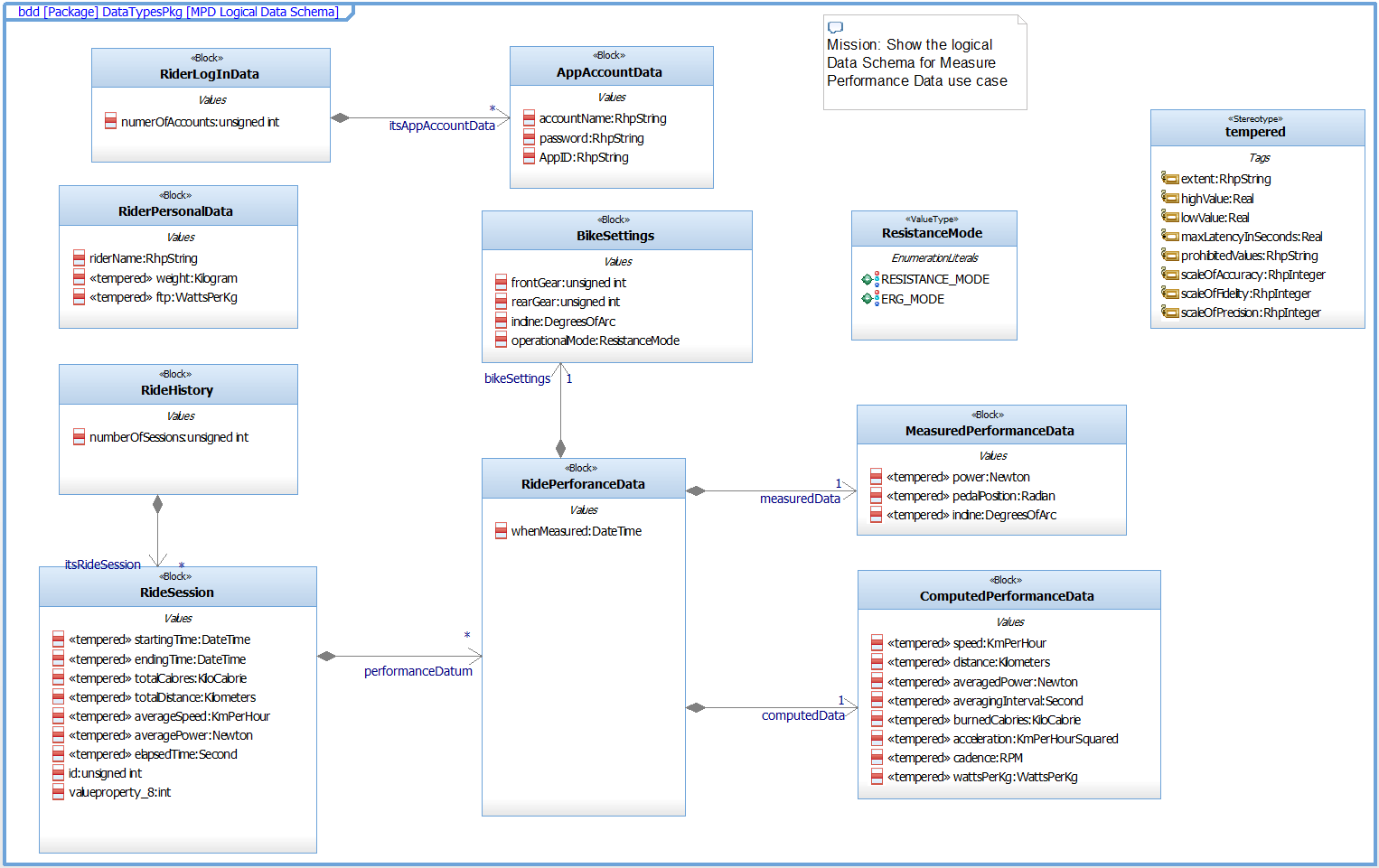


Figure 32: Data Schema

### Defining a Named Constant

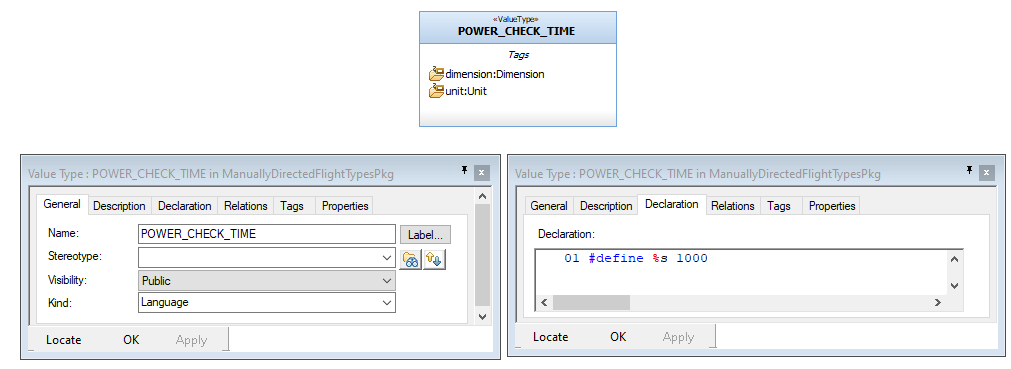


Figure 33: Defining a named Constant

## Modeling Trade Studies

Trade studies are a kind of architectural analysis and, if represented in the model, are expected to exist within subpackages of the ArchitecturePkg::ArchitecturalAnalysisPkg.

* Use parametric diagrams to perform trade studies or to represent computational constraint models
* Create a block that contains the raw *measures of effectiveness* (moe) as value properties
* Create constraint blocks to model the utility curve for the moes
* Create constraint blocks to model the weighted objective function

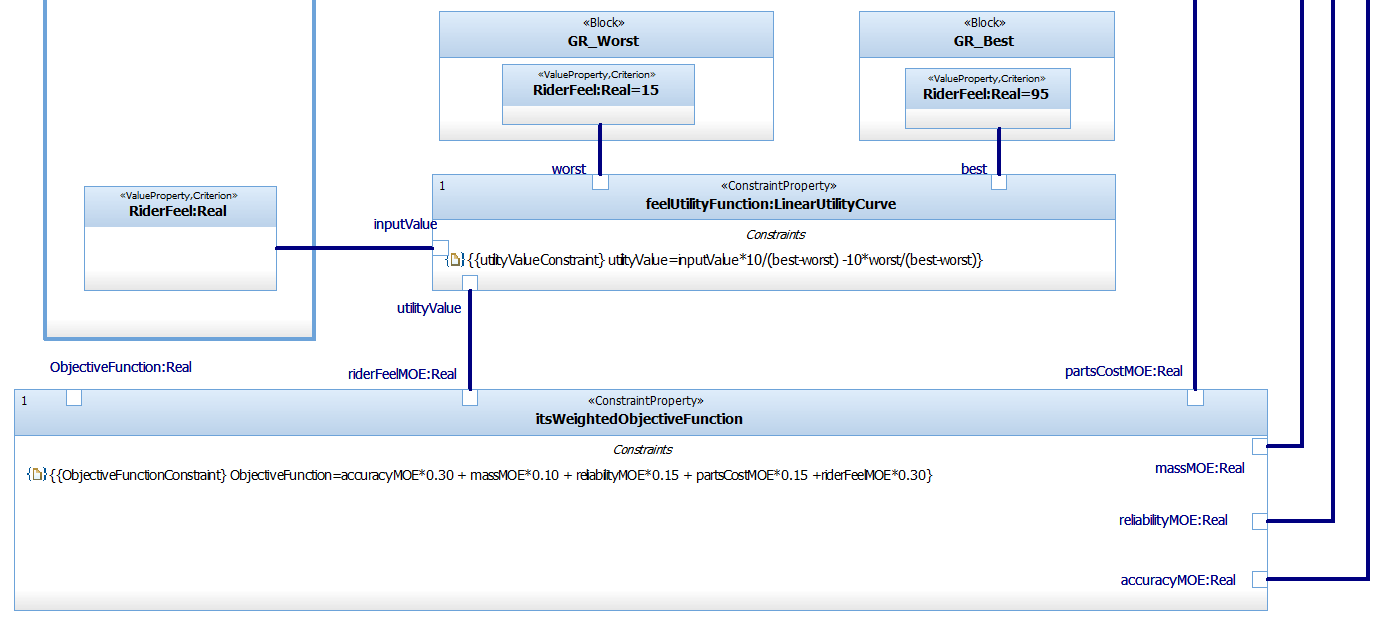


Figure 34: MOEs, Constraints, and Objective Functions

## Relating to ASPICE and ISO 26262

To support ASPICE, the following content and views – at minimum – will be contained within a systems model or model federation:

* Model Overview Diagram
* System Context Type
* System Connected Context
* System Composition Architecture
* System Connected Architecture
* Requirements-Architectural design elements trace matrix
* System Block state behavior identifying modes/primary system states and their transition
* State machines for the subsystems and indications of how they map to system states
* Activity and/or state diagrams depicting dynamic system behavior
* Sequence diagrams showing specific interactions (scenarios) of the architectural elements that is consistent with the state and activity models
* Interface diagram and/or tables showing the interface blocks and their properties (flow properties, event receptions, and functions invoked over the connections)
* Data schema
* Deployment architecture (BDD and IBD) with interdisciplinary interfaces)

The appropriate stereotypes from the Safety Profile will be applied to hold ASPICE and ISO 26262 model relevant metadata such as

* Capacity/memory needs
* ASIL Level
* Internally vs externally developed software
* Likelihood (such as for a fault)
* Severity (such as for a fault)
* Risk (such as for a fault)
* Fault Tolerance Time (such as for a fault)
* Worst case execution time (such as for a behavior)

## Safety Profile

This profile will contain elements to support both ASPICE and ISO26262 as well as providing some common table and matrix layouts.

All systems models will contain via reference, the Safety Profile. See **Safety Profile Reference Guide** for information on its use.

# References

**Automotive SPICE: Process Reference Model** Version 3.1 (November 2017)

**ISO 26262-6:2018: Road Vehicles – Functional Safety – Part 6: Product development at the software level** (2018)

**Safety Profile Reference Guide** by Dr. Bruce Powel Douglass (2020)

**Agile Model-Based Systems Engineering Cookbook** by Dr. Bruce Powel Douglass, (2021)

**Agile Systems Engineering** by Dr. Bruce Powel Douglass, (2016)

**Real-Time Agility** by Dr. Bruce Powel Douglass, (2009)

**Real-Time Agile Systems and Software Development** website [www.bruce-douglass.com](http://www.bruce-douglass.com)