

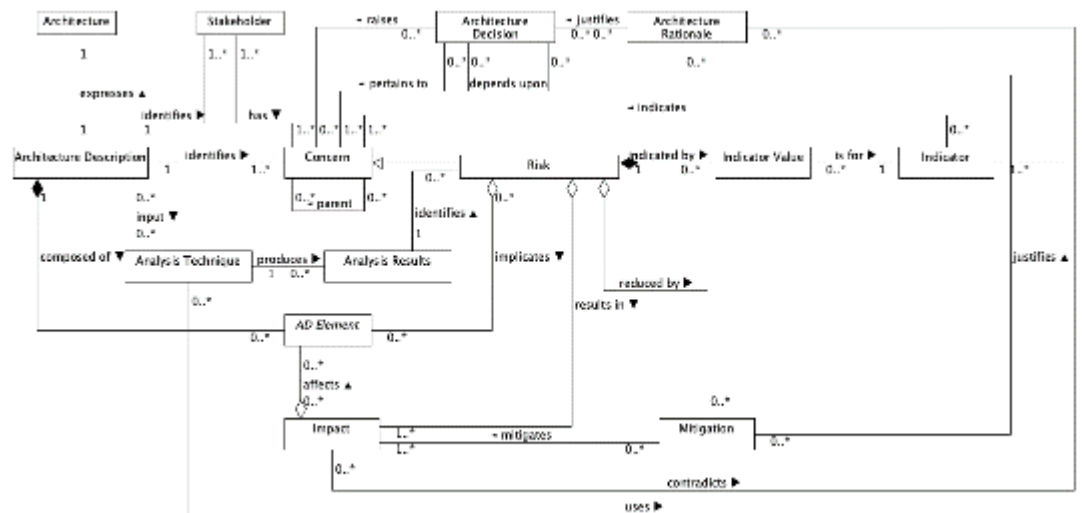
## Architecture Risk Model Research Questionnaire

### Section 1 – Participant Experience & Background

1. How many years of experience do you have in commercial software intensive systems engineering?  
0
2. How many years of experience do you have in commercial software development?  
20 years
3. How many years of enterprise architecture experience do you have?  
0
4. How many years of solution architecture experience do you have?  
0
5. How many years of technical architecture experience do you have?  
1
6. How many years of SysML experience do you have?  
0
7. How many years of UML experience do you have?  
10
8. How many projects have you worked on that have involved a SysML or UML model?  
3
9. How many years do you have working with waterfall development?  
15
10. How many years do you have working with agile (e.g. Scrum & SAFe) development?  
5

## Part 2 – Approach Background

The research is evaluating whether risks could be described using the following model that extends ISO 42010 – Architecture Descriptions:



ISO 42010 Concept	ISO 42010 Definition
AD element	"any construct in an architecture description." (p. 7)
Architecture	"fundamental concepts or properties of a system in its environment embodied in its elements, relationships, and in the principles of its design and evolution." (p.8)
Architecture Decision	"pertain to system concerns; however, there is often no simple mapping between the two. A decision can affect the architecture in several ways." (p. 7)
Architecture Description	"work product used to express an architecture." (p. 2)
Architecture Model	"uses modelling conventions appropriate to the concerns to be addressed." (p. 6)
Architecture Rationale	"records explanation, justification or reasoning about architecture decisions that have been made." (p. 7)
Architecture View	"work product expressing the architecture of a system from the perspective of specific system concerns." (p. 2)
Architecture Viewpoint	"work product establishing the conventions for the construction, interpretation and use of architecture views to frame specific system concerns." (p. 2)
Concern	"interest in a system relevant to one or more of its stakeholders." (p. 2)
Correspondence	"defines a relation between AD elements." (p. 7)
Correspondence Rule	"enforce relations within an architecture description (or between architecture descriptions)." (p. 7)
Model Kind	"conventions for a type of modelling." (p. 2)
Stakeholder	"individual, team, organization, or classes thereof, having an interest in a system." (p. 2)
System-of-interest	"systems that are man-made and may be configured with one or more of the following: hardware, software, data, humans, processes (e.g., processes for providing service to users), procedures (e.g. operator instructions), facilities, materials and naturally occurring entities." (p. 3)
Extension Concept	Extension Definition
Risk	Sub type of <b>Concern</b> that represents a <b>Risk</b> , e.g. error-proneness or security vulnerability.
Indicator	Indicates the relative risk of a <b>Risk</b> . An <b>Indicator</b> could be a quantitative software engineering metric such as a coupling measure or a qualitative assessment by an architect.
Indicator Value	The value of a particular <b>Indicator</b> for a particular <b>Risk</b> .
Impact	Represents a potential consequence of a <b>Risk</b> being left untreated.
Mitigation	Represents an action that could be taken to reduce the potential <b>Impact</b> of a <b>Risk</b> .
Analysis Technique	Identifies the architecture analysis technique used to for a risk analysis.
Analysis Results	Encapsulates the results of a risk analysis performed using an analysis technique.

## Part 3 – Approach Examples

### **Example 1 - Excessive Change Propagation**

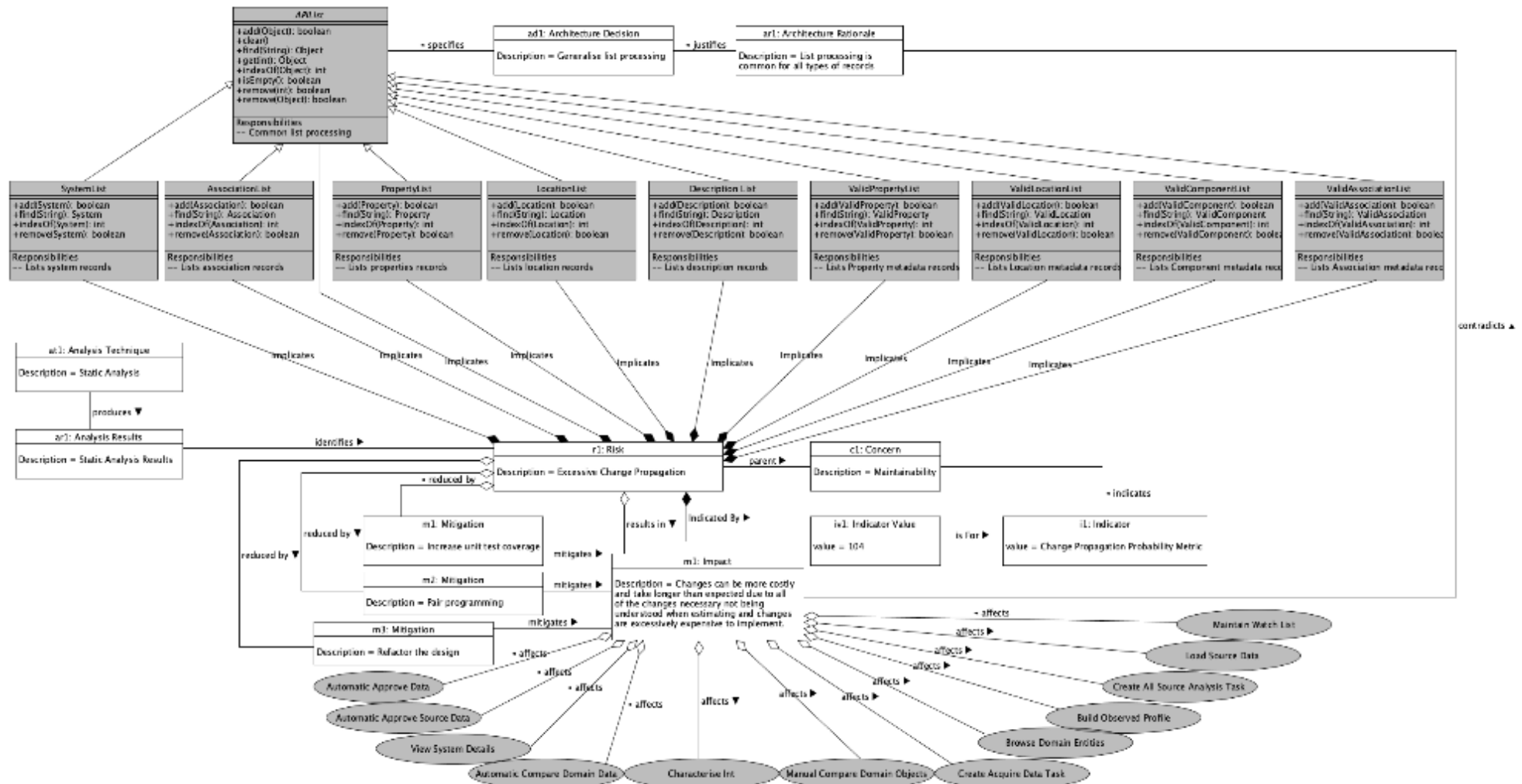
#### **Text Risk Description**

Title:	Excessive change propagation
Details:	Complex concrete sub-classes have emerged from the diverse use cases the lists had to support. E.g. SystemList needs “deleted record processing” whereas PropertyList does not. This causes conflicts between abstract class code and concrete sub-class code. This could be considered an unhealthy inheritance tree. There are also some common complex routines that are not always abstracted so when bugs have to be fixed sometimes many List sub-classes had to be changed.
Impact:	Changes can be more costly and take longer than expected due to all of the changes necessary not being understood when estimating and changes are excessively expensive to implement.
Mitigations:	Increase test coverage, pair programming, refactor the design

## Risk Model Representation

Notes:

- Grey background elements indicate elements from the design model;
- White background elements are elements added from the proposed risk model.



## Example 2 - 3<sup>rd</sup> Party Interface Changes outside of MASS control

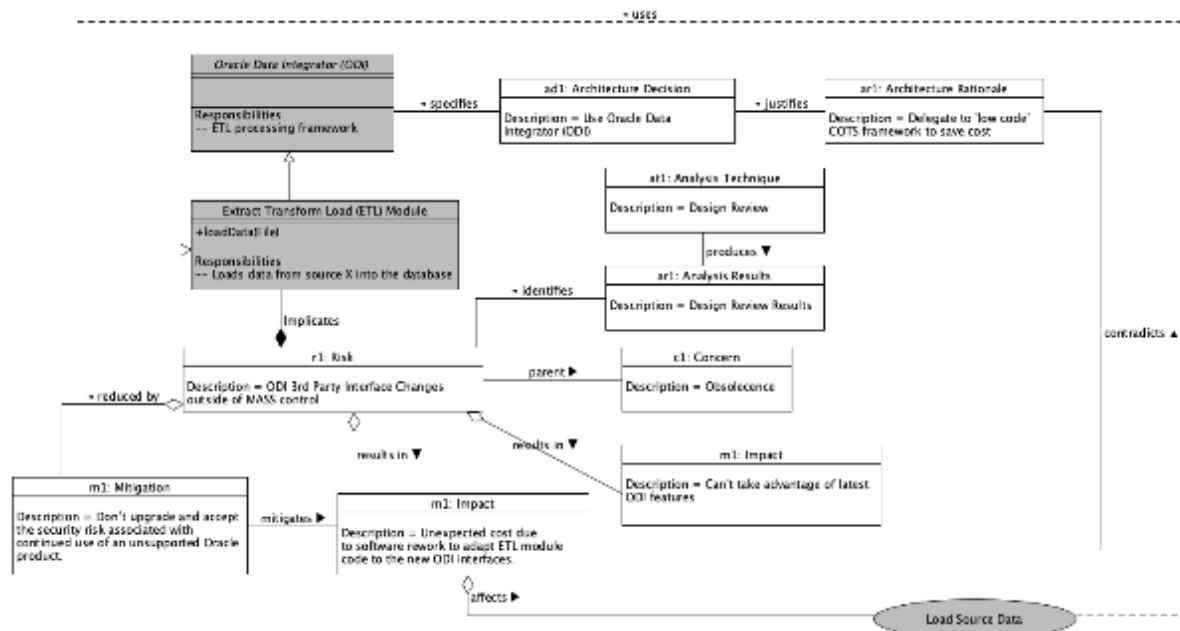
### Text Risk Description

**Title:** Low code framework Interface Changes outside of MASS control  
**Details:** Oracle Data Integrator (ODI) has changed its interface specification. This will require MASS code to be reworked if ODI has to be upgraded.  
**Impact:** Unexpected cost due to software rework to adapt ETL module code to the new ODI interfaces. Can't take advantage of latest ODI features.  
**Mitigation:** Don't upgrade and accept the security risk associated with continued use of an unsupported Oracle product.

### Risk Model Representation

Notes:

- Grey background elements indicate elements from the design model;
- White background elements are elements added from the proposed risk model.



Part 4 – Risk Model Evaluation Questions

#	Question	Answer (Delete Y / N / Not Sure as appropriate)			Comments – Please include any qualifying statements
		Waterfall	Agile e.g. Scrum	Scaled Agile e.g. SAFe	
11.	Do you think the proposed risk model would help design reviews?	Y / <u>N</u> / Not Sure	Y / N / <u>Not Sure</u>	Y / N / <u>Not Sure</u>	<i>(“Not Sure” marked for all Scaled Agile as no experience)</i> My concern would be constraining to a reasonable number of “what-if” scenarios for the design phase – I am assuming this is a diagram/model per risk
12.	Do you think the proposed risk model could help to identify risks?	Y / N / <u>Not Sure</u>	<u>Y</u> / N / Not Sure	Y / N / <u>Not Sure</u>	This could aid a deeper analysis of risk for waterfall (assuming this is used in analysis and design, before the coding).  The examples given lead to a better fit (and a more complete analysis) upon existing (iteratively produced) software that is due to change. Both pieces of example software are established and require a change or refactor – thus the analysis is easier.
13.	Do you think the proposed risk model could help the analysis of identified risks?	<u>Y</u> / N / Not Sure	<u>Y</u> / N / Not Sure	Y / N / <u>Not Sure</u>	
14.	Do you think the proposed risk model could help with the assessment of analysed risks?	<u>Y</u> / N / Not Sure	<u>Y</u> / N / Not Sure	Y / N / <u>Not Sure</u>	
15.	Do you think the proposed risk model could help the mitigation of assessed risks?	<u>Y</u> / N / Not Sure	<u>Y</u> / N / Not Sure	Y / N / <u>Not Sure</u>	
16.	Do you think the proposed risk model could help monitoring of ongoing risks?	Y / N / <u>Not Sure</u>	Y / N / <u>Not Sure</u>	Y / N / <u>Not Sure</u>	Updates to the model would hopefully mean a reduction in the complexity of the diagram (as mitigations are used) – though it could also reveal a new risk. The Oracle example is an <i>environmental</i> risk that is not really in your control – you can only react (but be ready for it with a

					robust and adaptable response, hopefully from the risk analysis)
17.	Do you think the proposed risk model could be useful when a design model doesn't exist?	Y / N / <u>Not Sure</u>	<u>Y</u> / N / Not Sure	Y / N / <u>Not Sure</u>	Using the risk model in place of design would be a good fit for a scenario where there is a "legacy black box" that has little-to-no-design that lives deeply rooted in a complex enterprise application (e.g. a banking model)
<b>#</b>	<b>Question</b>				<b>Answer – Please justify your answer with a brief explanation</b>
18.	What do you think might be the advantages and disadvantages of modelling the risk in this way?				<p>Advantage – it's more analysis and it is detailed. I interpret that certain 'boxes' are mandatory (?) – so this is a framework that ensures that mandatory aspects of a risk are identified e.g. Analysis Technique; Analysis Results; Risk; Mitigation; Impact</p> <p>Disadvantage – discipline required as too many "mitigations" leads to a complex diagram – or (as shown) an "impact" affects many things. Therefore the diagram would ideally needs breaking down...</p>
19.	Which approach (textual description or the proposed risk model) do you prefer and why?				<p>I prefer the diagram <i>with</i> the text. It gives a brief overview of what I am looking at.</p> <p>The text alone (especially if bullet-pointed or numbered) is more concise, which is preferable if you need to convey things quickly.</p>
20.	Do you think any of the entities or associations in the proposed model are unnecessary or overkill, if so which ones?				The sources and justification of the risk – embodied in the Stakeholder and the Analysis Technique and Analysis Results could be out of scope if we just want to model the risks and their mitigations.
21.	Can you think of any entities or associations that are missing from the proposed risk model?				I would propose that the "Architecture View" concept is used to partition the overall risk modelling (or as a container) – See

		Answer 22.
22.	Do you have any other feedback about the proposed risk model or its usage?	Separation of history (Stakeholders, Concerns, Analysis and Analysis Results) from the Risks, Mitigations and Impacts by utilising the Architecture Views concept would facilitate a suite of risk analysis with a separate history <i>component</i> should implementers wish to investigate; likewise the analysts may not wish to go as far as how the problem is eventually fixed (thus they are only interested in the Concerns and Analysis with the Stakeholder)