

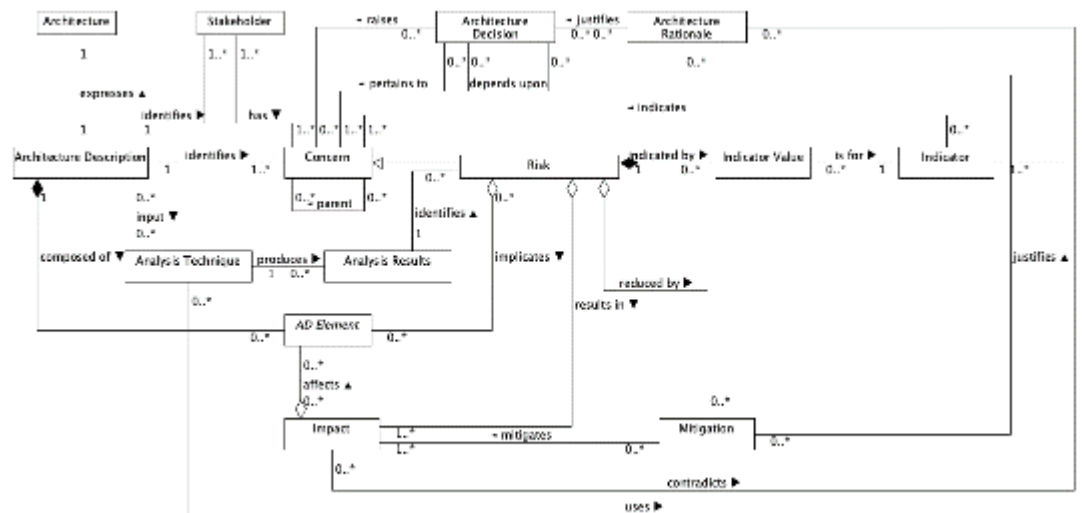
## Architecture Risk Model Research Questionnaire

### Section 1 – Participant Experience & Background

1. How many years of experience do you have in commercial software intensive systems engineering?  
12 years
2. How many years of experience do you have in commercial software development?  
N/A – Non Software Developer
3. How many years of enterprise architecture experience do you have?  
No in depth Enterprise Architecture Experience
4. How many years of solution architecture experience do you have?  
7 Years
5. How many years of technical architecture experience do you have?  
7 Years
6. How many years of SysML experience do you have?  
5 Years
7. How many years of UML experience do you have?  
10 Years
8. How many projects have you worked on that have involved a SysML or UML model?  
12
9. How many years do you have working with waterfall development?  
7 Years
10. How many years do you have working with agile (e.g. Scrum & SAgE) development?  
4 Years

## 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**

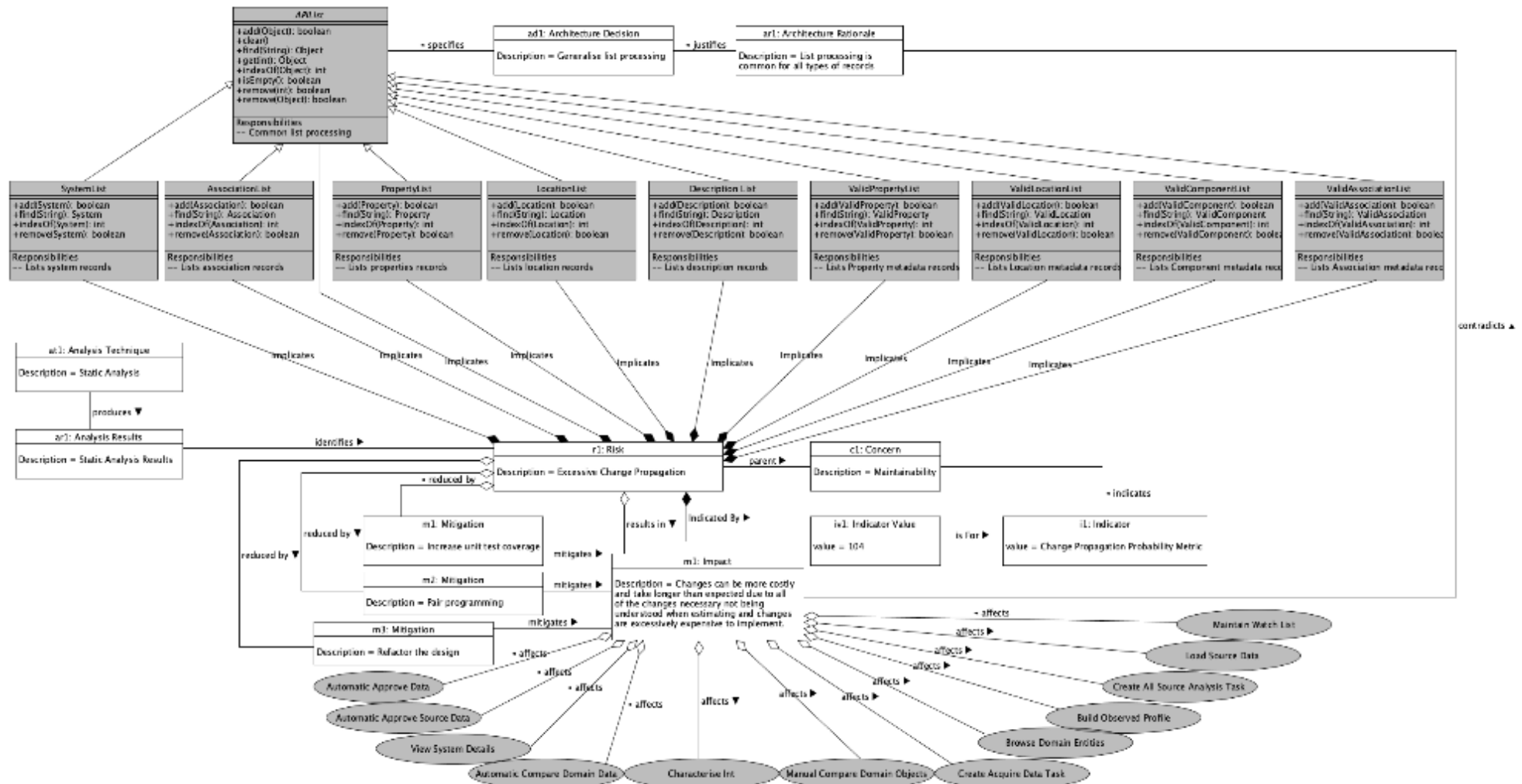
#### **Text Risk Description**

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

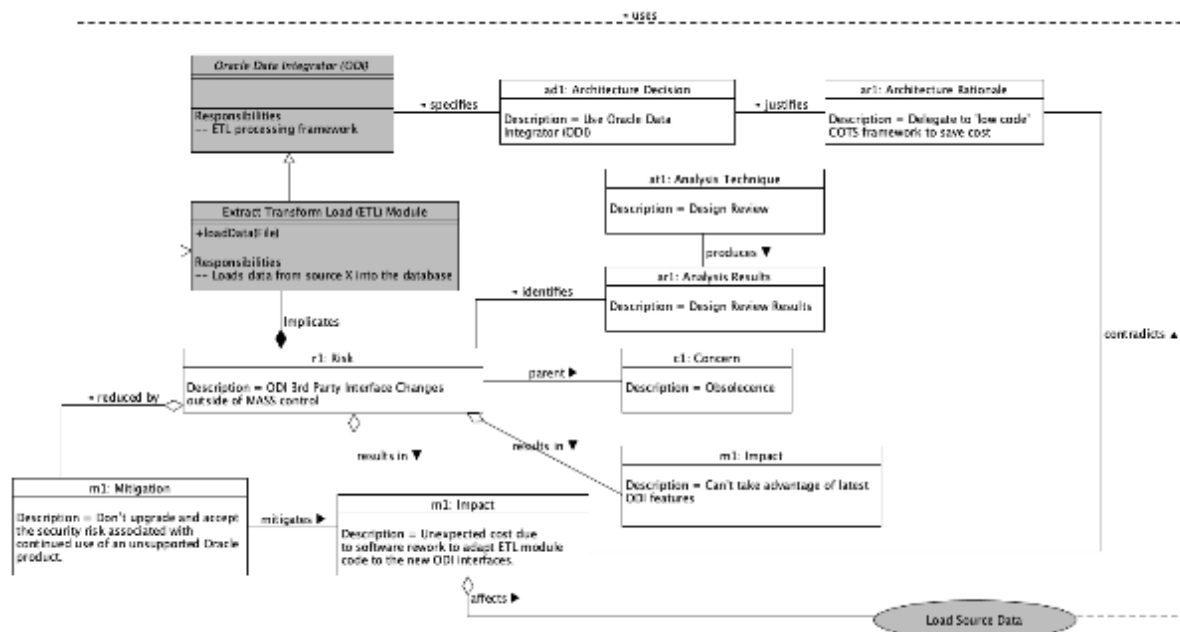
### Text Risk Description

**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	N	Y	To generate the models in sufficient detail has a higher overhead than a traditional “risk register” – but clearly imparts significantly more information. I think this would be ideal for waterfall and Scaled Agile projects but may no align so easily with an agile approach (primarily based on time/effort to produce). Design reviews will benefit from a clear link to architecture design and associated risk.
12.	Do you think the proposed risk model could help to identify risks?	Y	Y	Y	Interesting question. Project risks change through the life-cycle of the project. A model based approach provides a risk <i>baseline</i> which can will develop as the project progresses. The very nature of MBSE will probably enable the identification of risks as the model matures. You will be able to understand the relationship to architecture and risk. So yes, I think where it is used it can be useful to identify risks.
13.	Do you think the proposed risk model could help the analysis of identified risks?	Y	Y	Y	Using a model-based approach will definitely enable the analysis of risks.
14.	Do you think the proposed risk model could help with the assessment of analysed risks?	Y	Y	Y	
15.	Do you think the proposed risk model could help the mitigation of assessed risks?	Y	Y	Y	It would enable the development of mitigations to risks as risk impact is clear.
16.	Do you think the proposed	Y	Y	Y	Models enable reports to be generated and the status of risks to

	risk model could help monitoring of ongoing risks?				be tracked, and their impact on the wider system to be understood.
17.	Do you think the proposed risk model could be useful when a design model doesn't exist?	Not Sure	Not Sure	Not Sure	I think you <i>could</i> use a model such as the one proposed, but it may have limited value if it can't be linked back into architectural design.
#	Question	Answer – Please justify your answer with a brief explanation			
18.	What do you think might be the advantages and disadvantages of modelling the risk in this way?	<p>Advantages: Clear view of risk and how impacts and mitigation can be traced back into the architectural model.</p> <p>Disadvantages:  I think primarily overhead in generating the models. It also requires an understanding of model-based systems/software engineering. Risk is often the responsibility of a non-specialist Project manager.</p> <p>Text based approach is also very quick to read – you can quickly understand the risk and mitigation, but the context to the wider design is not available.</p>			
19.	Which approach (textural description or the proposed risk model) do you prefer and why?	<p>I prefer the model but can see that the output from the model will ultimately end up being a textural description. This is probably no bad thing – different project stakeholders require information presented to them in different ways.</p>			

Andrew Leigh, Michel Wermelinger, Andrea Zisman

20.	Do you think any of the entities or associations in the proposed model are unnecessary or overkill, if so which ones?	No
21.	Can you think of any entities or associations that are missing from the proposed risk model?	Impact could specify <i>cost, effort, delay, capability loss</i> etc as attributes? They could also be split out further as entities? Benefits could be that reports could be generated that show the project financial impact of risks, or time delays etc vs textural descriptions. (But the proposed model will support that I suspect depending on the language used)
22.	Do you have any other feedback about the proposed risk model or its usage?	It will require “buy in” from the normal project risk holders, but technically I think this is great approach to a very important area of software/system Engineering.