

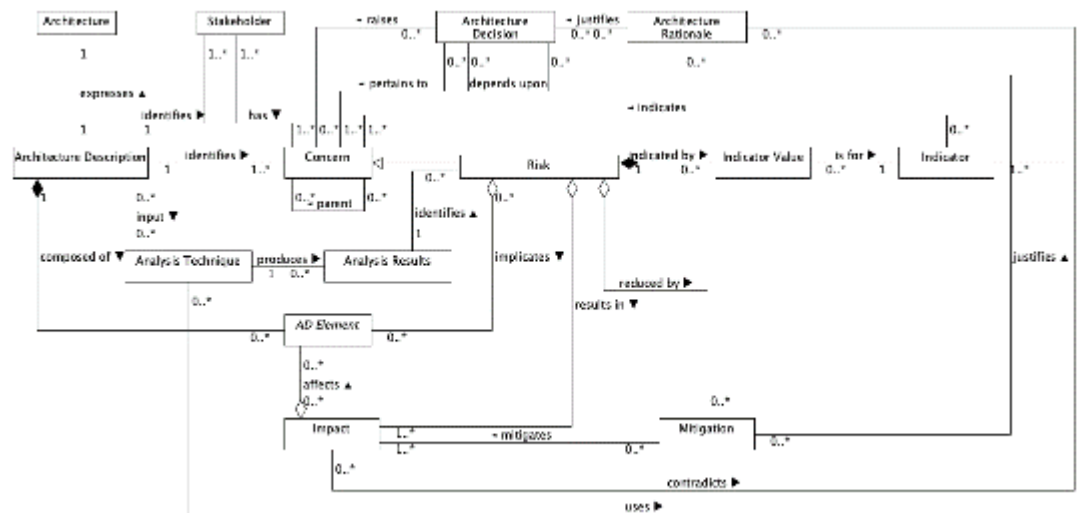
## Architecture Risk Model Research Questionnaire

### Section 1 – Participant Experience & Background

1. How many years of experience do you have in commercial software intensive systems engineering?  
7
2. How many years of experience do you have in commercial software development?  
17
3. How many years of enterprise architecture experience do you have?  
0
4. How many years of solution architecture experience do you have?  
10
5. How many years of technical architecture experience do you have?  
17
6. How many years of SysML experience do you have?  
1
7. How many years of UML experience do you have?  
15
8. How many projects have you worked on that have involved a SysML or UML model?  
5
9. How many years do you have working with waterfall development?  
17
10. How many years do you have working with agile (e.g. Scrum & SAFe) development?  
Scrum 5, SAFe 0

## 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**

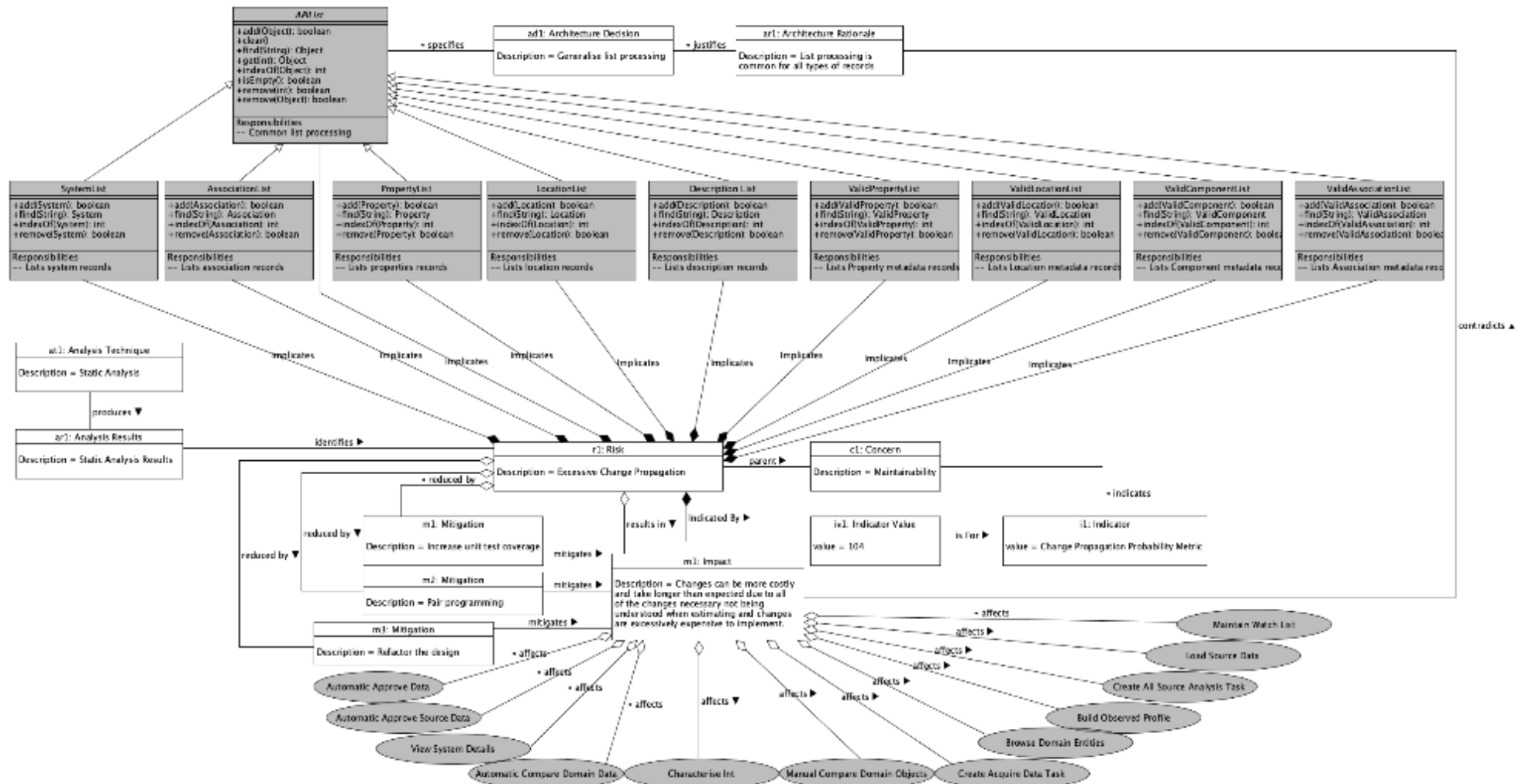
#### **Text Risk Description**

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

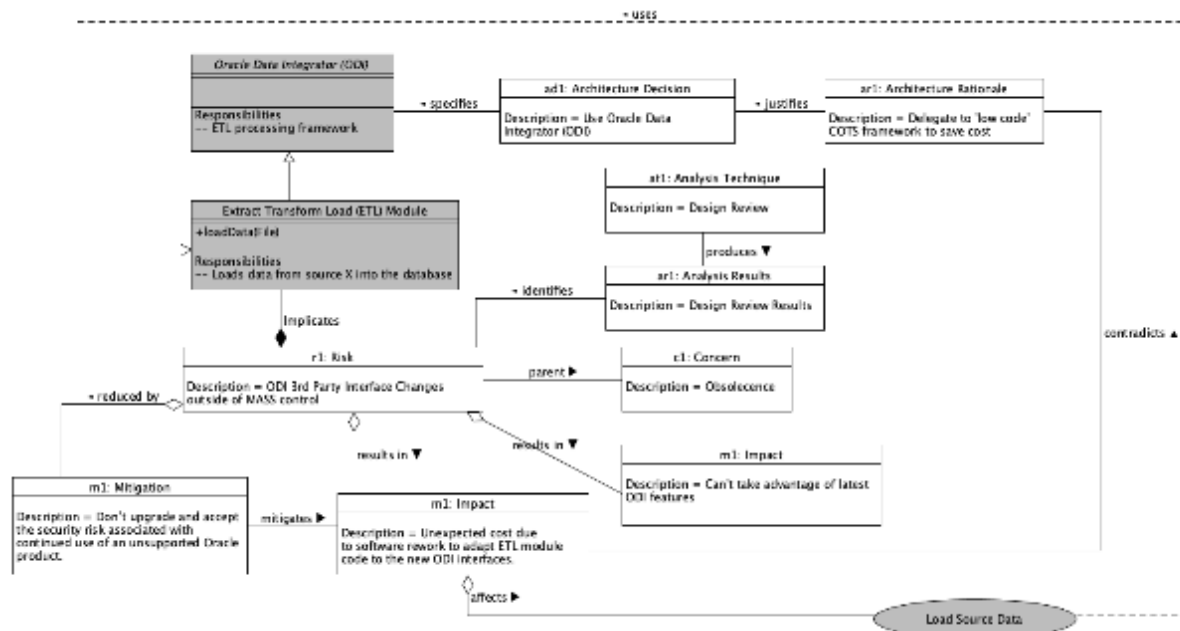
### Text Risk Description

**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

For all questions in the following table, I'm not sure that the model would be a good fit for agile – its manifesto valuing a working product over comprehensive documentation.

For all questions in the following table, I have no experience of SAFe so don't feel able to comment meaningfully.

#	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	Not Sure	Y / N / Not Sure	With supporting documentation to assist the reviewers, e.g. a list of standard risks that should be considered.
12.	Do you think the proposed risk model could help to identify risks?	Not Sure	Not Sure	Y / N / Not Sure	I think the review process would help identify risks, I see the model more as a means of ensuring that required details are addressed.
13.	Do you think the proposed risk model could help the analysis of identified risks?	Y	Not Sure	Y / N / Not Sure	Definitely, especially with some software tooling.
14.	Do you think the proposed risk model could help with the assessment of analysed risks?	Y	Not Sure	Y / N / Not Sure	As above.
15.	Do you think the proposed risk model could help the mitigation of assessed risks?	Y	Not Sure	Y / N / Not Sure	Through identifying mitigation on a per-risk basis. Supporting documentation, e.g. proven mitigation factors for particular risk categories.
16.	Do you think the proposed risk model could help monitoring of ongoing risks?	Y	Not Sure	Y / N / Not Sure	With a recorded status for each risk that is kept up to date as mitigation is applied, indicators change and so on.
17.	Do you think the proposed risk model could be useful when a design model doesn't exist?	Y	Y	Y / N / Not Sure	To assist in the comparison of possible design models from a risk perspective.

#	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?	Advantages: Unambiguous description of the risk. Model provides a design for a software application to manage risk aspects – way better than an Excel spreadsheet. Disadvantages: Participants need some relevant experience to understand the model and the modelling language.
19.	Which approach (textural description or the proposed risk model) do you prefer and why?	I prefer the risk model, as I am a visual learner. The model has a “syntax” that provides more precision than a purely textual description. The model provides explicit relationships between data items.
20.	Do you think any of the entities or associations in the proposed model are unnecessary or overkill, if so which ones?	No, they all appear relevant and are needed for a complete description of risk in a well-engineered system
21.	Can you think of any entities or associations that are missing from the proposed risk model?	I think the only things I identified, such as overall risk score, impact score, likelihood and safety / security criticality could all be covered as Indicators. Perhaps some indicators should be specified and made mandatory, while optional indicators could be generalised. Perhaps cost of mitigation should be included to allow cost/benefit analysis to be calculated on a per-risk basis.
22.	Do you have any other feedback about the proposed risk model or its usage?	I like it – it makes sense and could be extended to cover other non-functional areas of architecture design.