

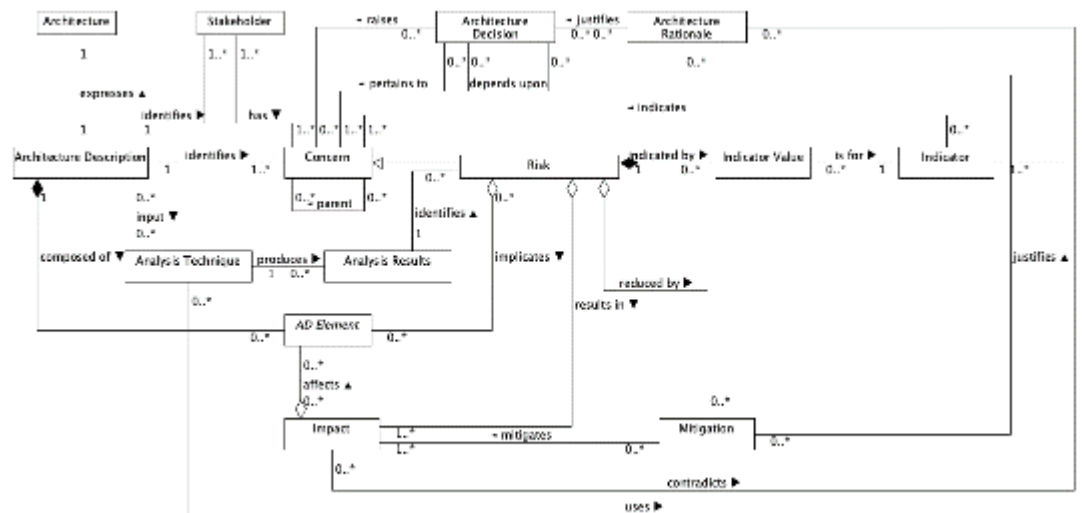
Architecture Risk Model Research Questionnaire

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?
17 years.
3. How many years of enterprise architecture experience do you have?
6
4. How many years of solution architecture experience do you have?
6
5. How many years of technical architecture experience do you have?
10
6. How many years of SysML experience do you have?
0
7. How many years of UML experience do you have?
13
8. How many projects have you worked on that have involved a SysML or UML model?
1
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?
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 Concern that represents a Risk , e.g. error-proneness or security vulnerability.
Indicator	Indicates the relative risk of a Risk . An Indicator 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 Indicator for a particular Risk .
Impact	Represents a potential consequence of a Risk being left untreated.
Mitigation	Represents an action that could be taken to reduce the potential Impact of a Risk .
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

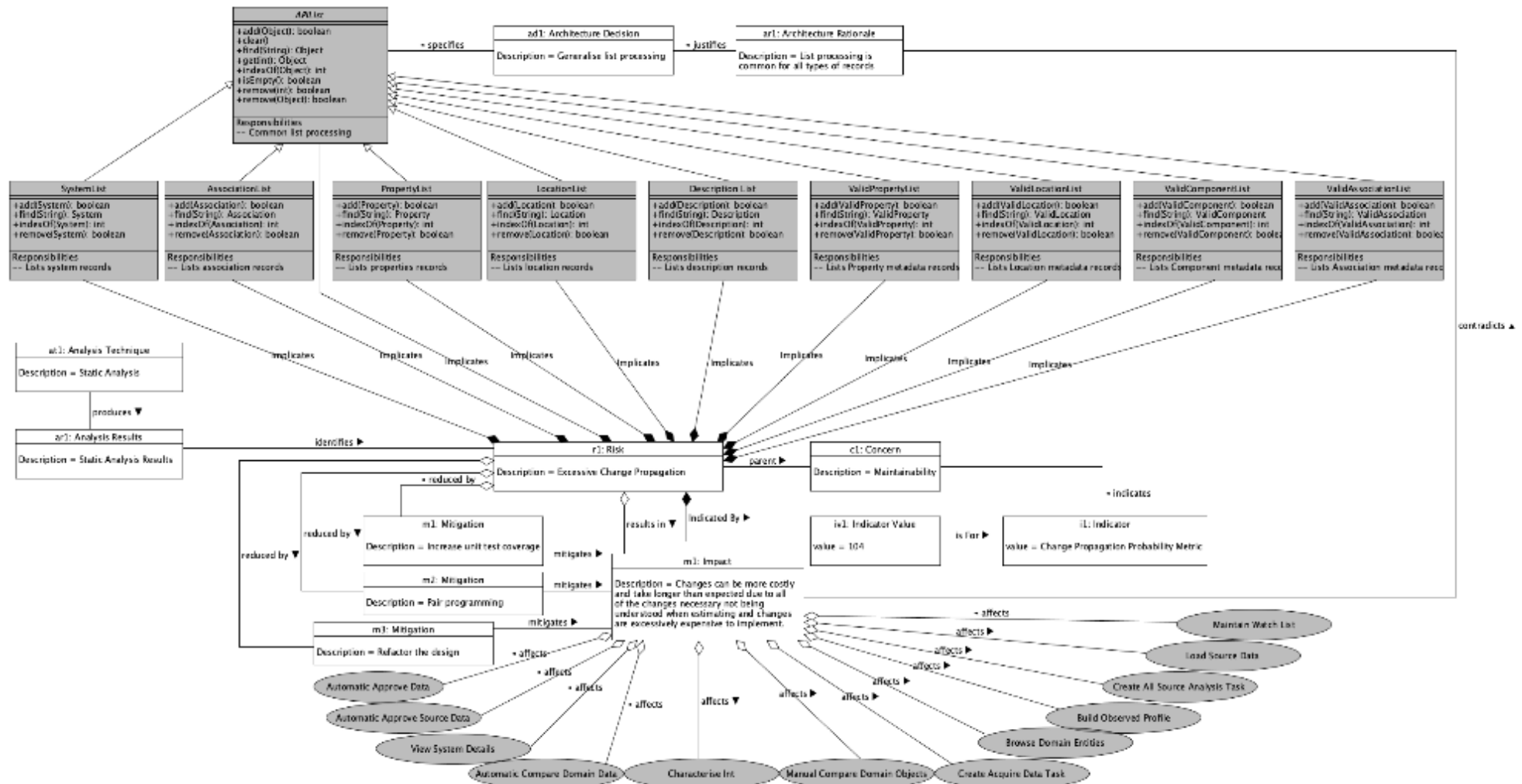
Text Risk Description

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 - 3rd Party Interface Changes outside of MASS control

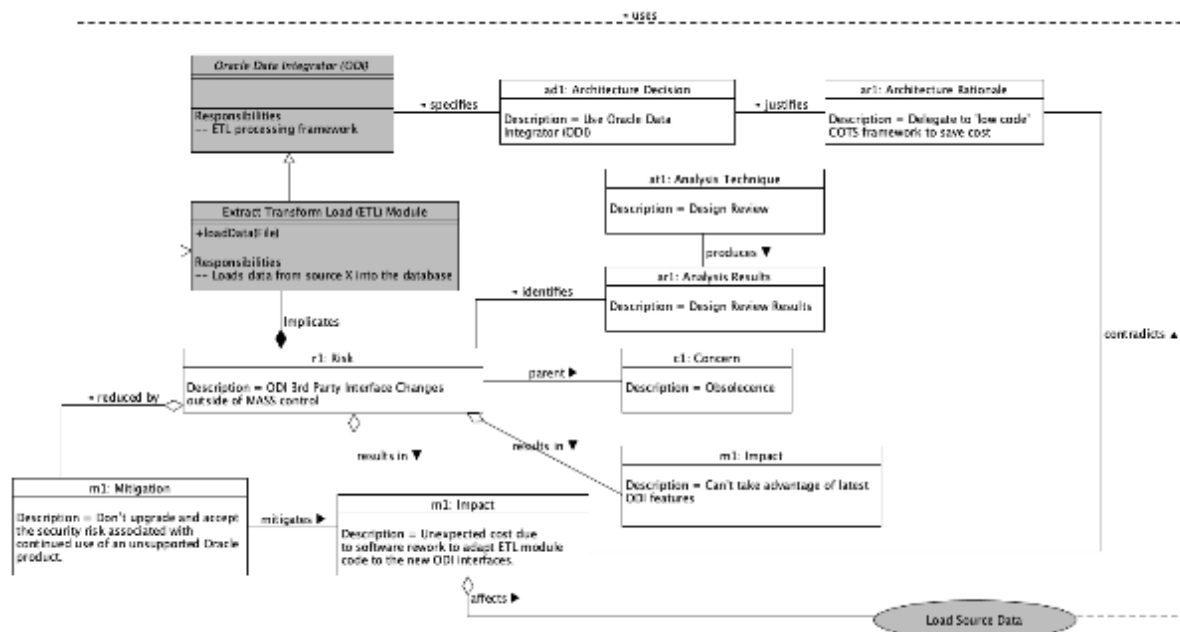
Text Risk Description

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. SAgE	
11.	Do you think the proposed risk model would help design reviews?	Y	Y	Y	It may be more effective with regular integrative architecture and design approach. Risks etc are more often dynamic over time, and can come and go as a project progresses.
12.	Do you think the proposed risk model could help to identify risks?	Y	Y	Y	It can clearly be used to gather risks that are refined around architecture styles, and balancing this with meeting requirements. Certain design patterns used carry specific risks, as highlighted in the example above. A single model may not be enough. Various stages of a software project may need the model to be slightly altered. The inclusion of Events when risks have happened would allow better analysis and mitigations. Further understanding of the reasons, the event happening also provide information about the risk.
13.	Do you think the proposed risk model could help the analysis of identified risks?	Y	Y	Y	It clearly can be used from a treatability point of view to see the path to the identification of a specific risk. This would aid further analysis of the risk, as well as enabling better communication, and understanding around the risk.
14.	Do you think the proposed risk model could help with the assessment of analysed risks?	Y	Y	Y	Again traceability and reasoning are all captured so yes. Without doubt domain knowledge and heuristics would also play a potentially larger part. The model could guide the choice of team to make the assessment.

15.	Do you think the proposed risk model could help the mitigation of assessed risks?	Y	Y	Y	Again traceability and reasoning are all captured so yes. Without doubt domain knowledge and heuristics would also play a potentially larger part. The model could guide the choice of team to make the mitigation assessment. Here other knowledge around fiancé etc could also play a large part.
16.	Do you think the proposed risk model could help monitoring of ongoing risks?	Not Sure	Not Sure	Not Sure	Not sure all the information is present for continual monitoring of risks. Another model may be better suited.
17.	Do you think the proposed risk model could be useful when a design model doesn't exist?	Y	Y	Y	Not all risks are associated with design. Modelling of risk should start from day 1 of a project. Assumptions made prior to high level architecture models still will have risk associated with them. As Architecture flows into design and into implementation the model has uses for selecting appropriate design and code patterns.
#	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>Provide a uniform process across many projects. This enables clear communication and understanding.</p> <p>Structured Training paths.</p> <p>Could provide Data Analysis through data mining over time and different projects. (Aids continual improvement)</p> <p>Disadvantages</p> <p>May be over complex for smaller short-lived projects.</p> <p>May not fit every project, may need tailoring.</p>			

19.	Which approach (textural description or the proposed risk model) do you prefer and why?	Hard to say they both back each other up, for a better understanding.
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?	<p>Risk Groups – I'm sure risks can be grouped, into different groups. The relationship would need to be many to many.</p> <p>Events – The occurrences of the risk happening. Linked to risk, mitigation (lightly (why did mitigation fail)) and impacts, both actual (occurred) and analysed (expected)</p> <p>Cost – Linked to mitigation. Many mitigations impose some sort of cost.</p> <p>Risks linked to other risks – Risks can be associated with other risks. E.g. Through increased likely hood after risk another risk has occurred etc.</p>
22.	Do you have any other feedback about the proposed risk model or its usage?	A lot of the information that would be stored in the model, may exist elsewhere in project documentation etc. How does this model link with the source of information to ensure a single source of truth is maintained?