

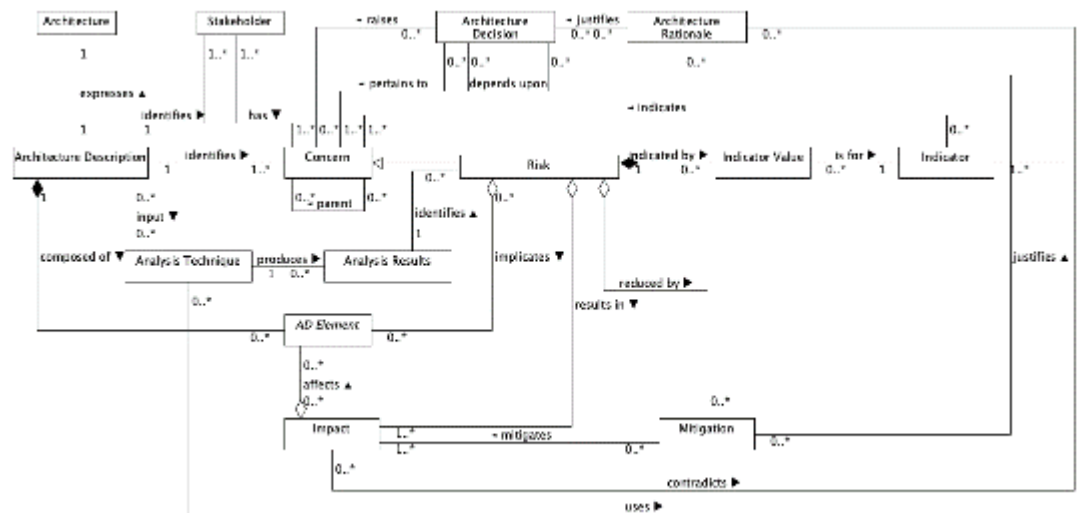
Architecture Risk Model Research Questionnaire

Section 1 – Participant Experience & Background

1. How many years of experience do you have in commercial software intensive systems engineering?
None, mainly system engineering.
2. How many years of experience do you have in commercial software development?
None.
3. How many years of enterprise architecture experience do you have?
4.
4. How many years of solution architecture experience do you have?
3.
5. How many years of technical architecture experience do you have?
3.
6. How many years of SysML experience do you have?
3.
7. How many years of UML experience do you have?
3.
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?
3.
10. How many years do you have working with agile (e.g. Scrum & SAFe) development?
3.

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

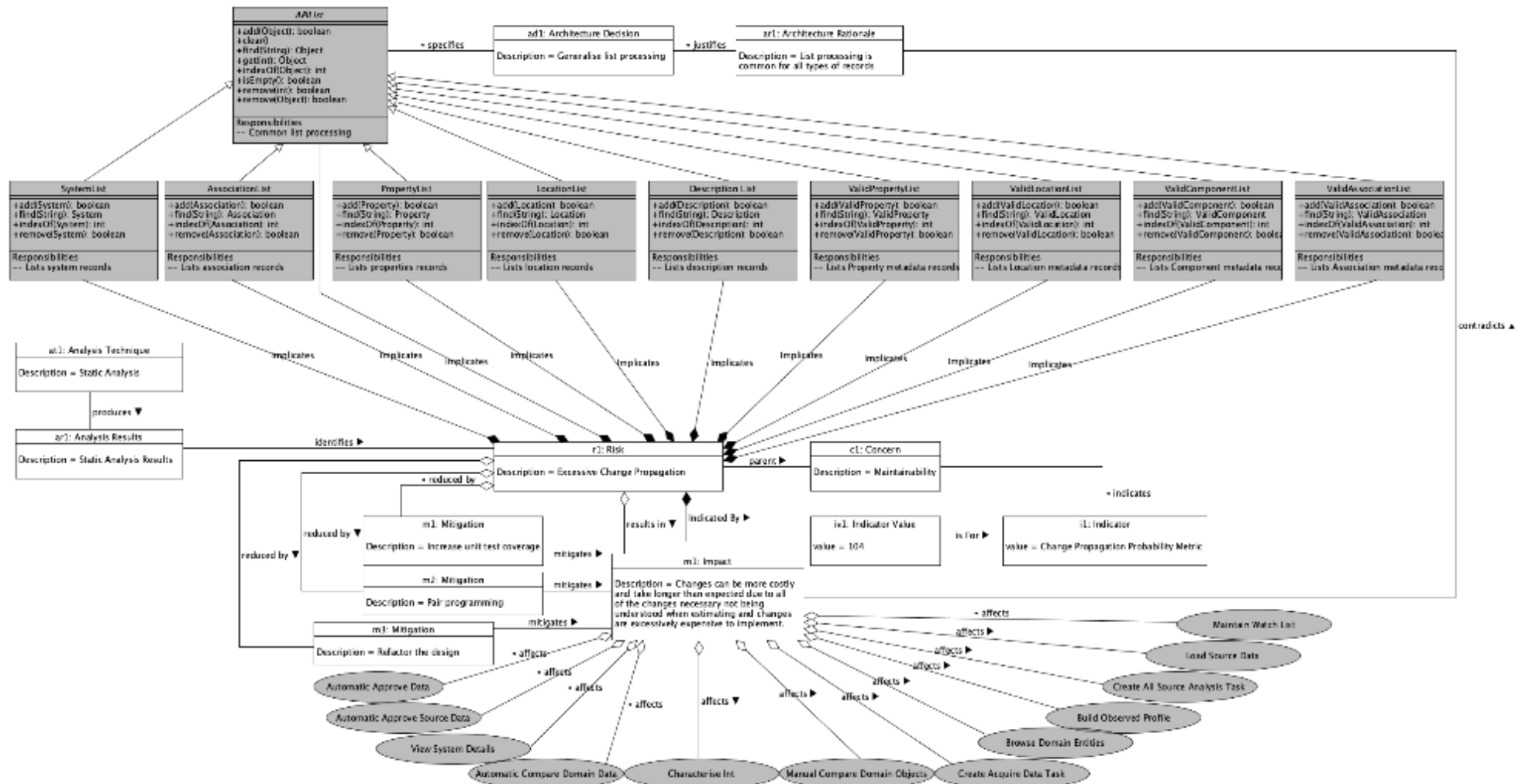
Text Risk Description

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:

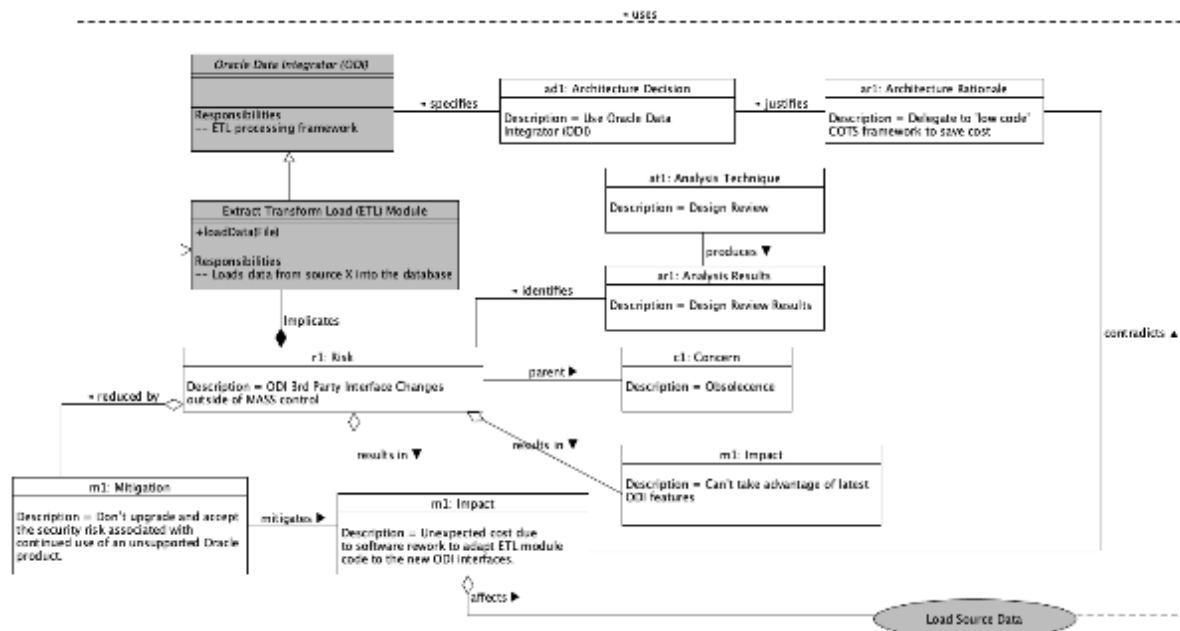
- Grey background elements indicate elements from the design model;
- White background elements are elements added from the proposed risk model.



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.

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. SAgile	
11.	Do you think the proposed risk model would help design reviews?	Y	Y	Y	<p>I believe that modelling will always assist in design reviews and the proposed risk model certainly visually frames risk concerns very well and includes the right risk analysis attributes (such as mitigation, analysis technique etc). The model will help inform the decision-making process when selecting the right course of action.</p> <p>I think that there are a couple of challenges; these being:</p> <ul style="list-style-type: none"> • Risk Perception - meaning that the risk mitigation from one stakeholder viewpoint may be different to that of another. This would probably necessitate the need to model alternative mitigations to show the impact of each course of action. • Treating the Concern element. In example 2, obsolescence is identified as the concern however, the mitigation affects system functionality. I wonder if there needs to be a direct relationship to a mitigation for the concern element? I think that if we had a way of categorising if the concern still remains post mitigation, or solved, then it would allow management, monitoring or later remedial action as part of the risk management process.
12.	Do you think the proposed risk model could help to identify risks?	Not Sure	Not Sure	Not Sure	<p>I think that the risk model will help to understand the risk but not necessarily identify the risks. I think that the identification of risk sits outside of the proposed risk model, however the risk model will provide the means to assess the risk and the impact to the system.</p>

13.	Do you think the proposed risk model could help the analysis of identified risks?	Y	Y	Y	Yes, I think that the risk model will be a useful aid assessing the magnitude of the risk, the appropriate treatment, or mitigation as it will force the system architect to model the risk and the outcomes. Having the system modelled will allow the architect the necessary visibility of interfaces, interactions, dependencies, constraints etc to make faster risk analysis.
14.	Do you think the proposed risk model could help with the assessment of analysed risks?	Y	Y	Y	Yes, particularly if using modelling and simulation within the model.
15.	Do you think the proposed risk model could help the mitigation of assessed risks?	Y	Y	Y	Yes, and allow the selection and assessment of mitigation alternatives.
16.	Do you think the proposed risk model could help monitoring of ongoing risks?	Y	Y	Y	<p>It could be a useful aid in the ongoing monitoring of risk and the impact to a recorded risk during assessment of change to the system. This would allow a more accurate and dynamic risk monitoring process however there would be the need to ensure that all risks pertaining to the system were accurately modelled.</p> <p>In terms of monitoring of ongoing risks, the neat thing to do would be to bring the system risks into one view (say on a Class diagram) and extend out the relationships to visualise the affected elements. What I mean by that is that you may have a risk on one diagram that also features in another view. By bringing the risk into a single "Risk Monitoring" view, you would be able to ensure that you are aware of the traceability to all project elements.</p>
17.	Do you think the proposed risk model could be useful when a design model doesn't exist?	N	N	N	If a design model doesn't exist, I'm not sure that there would be sufficient information available to make an accurate analysis or decision with the risk model alone. I think you really need that traceability between system elements to be sure that the right mitigations or treatment are put in place.

#	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>The main advantage is that you will be able to make the most accurate decisions around risk versus other means, understand the impact of risk and manage risk more effectively.</p> <p>Can't really see too many disadvantages other than maybe the cost involved in modelling risk? Or, if a system architect did not model all available mitigations and steered the model from the wrong risk perspective perhaps?</p> <p>There is a risk that the risk model could get extremely complicated in a real-life scenario making it difficult to comprehend.</p>
19.	Which approach (textual description or the proposed risk model) do you prefer and why?	<p>The first one as it has Indicator and Indicator Value to specify the relative risk.</p> <p>It's not clear on example 1 though if M1, M2 and M3 mitigations are all needed, which is the most effective or most desirable.</p>
20.	Do you think any of the entities or associations in the proposed model are unnecessary or overkill, if so which ones?	No, all seems perfectly logical and appropriate.
21.	Can you think of any entities or associations that are missing from the proposed risk model?	I think that we need some form of control entity for the Concern object. This will ensure that whilst we may mitigate a risk, the Concern does not get overlooked.
22.	Do you have any other feedback about the proposed risk model or its usage?	Other than it would be good to workshop this as a group! Very interesting concept.