

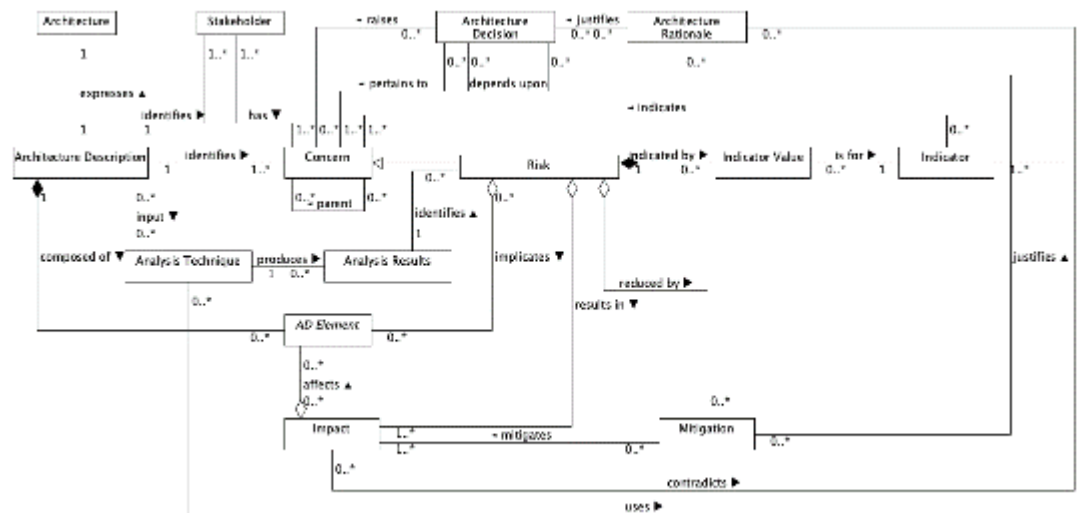
Architecture Risk Model Research Questionnaire

Section 1 – Participant Experience & Background

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

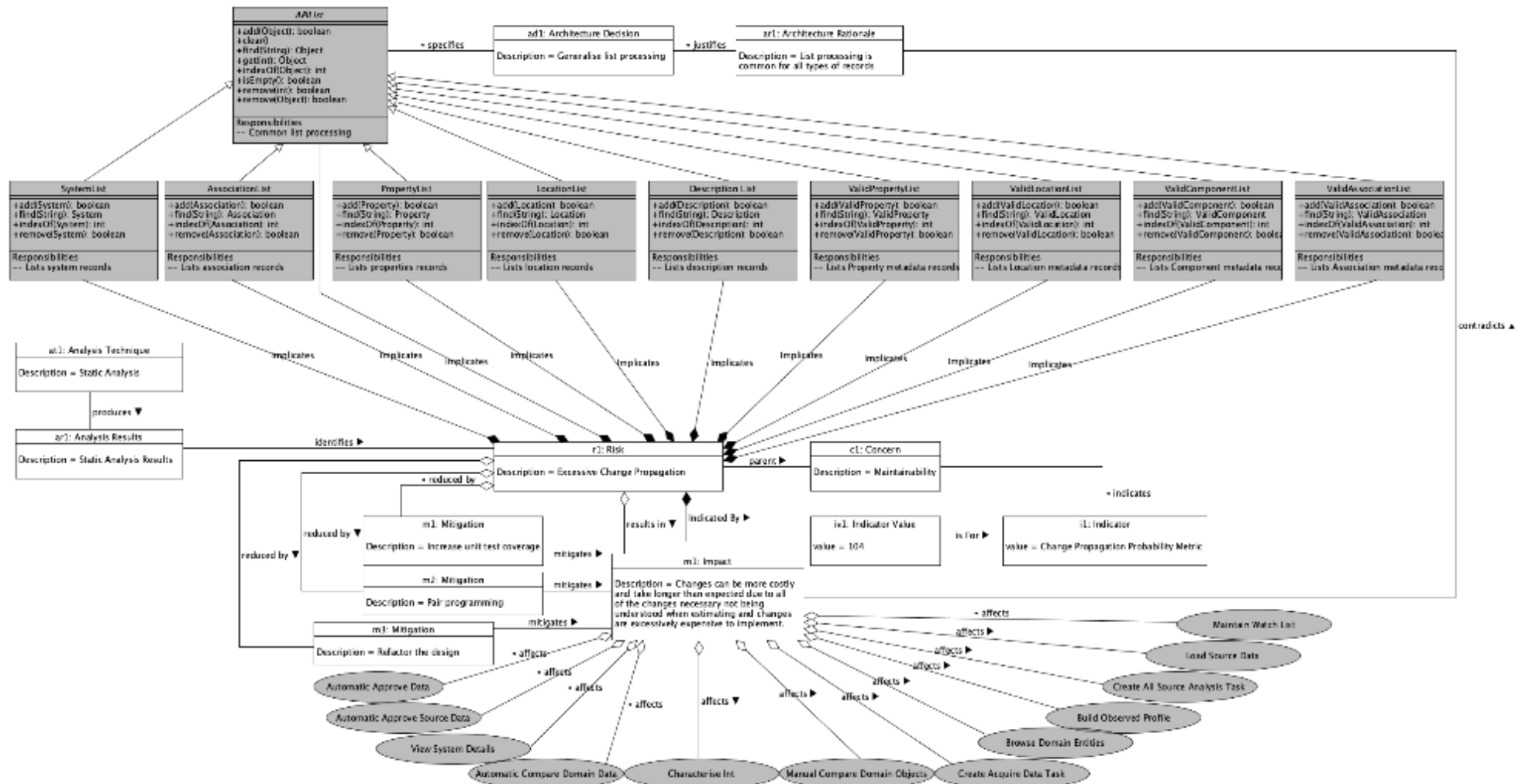
Text Risk Description

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:

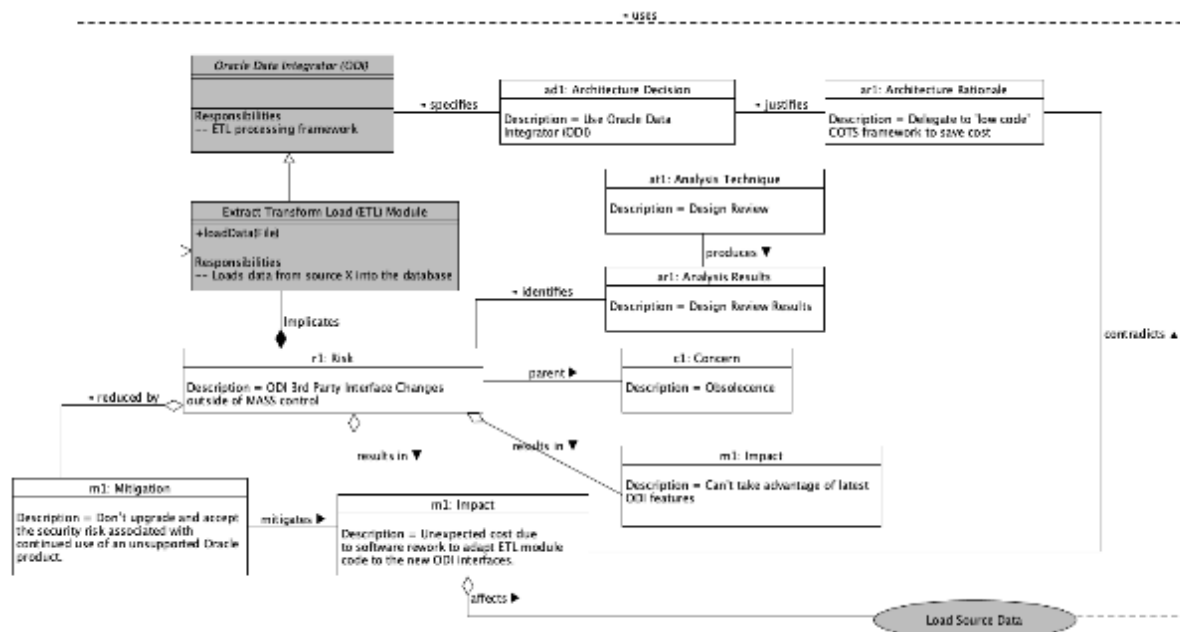
- Grey background elements indicate elements from the design model;
- White background elements are elements added from the proposed risk model.



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. SAgE	
11.	Do you think the proposed risk model would help design reviews?	Y / N / Not Sure	Y / N / Not Sure	Y / N / Not Sure	I believe the delivery approach has no direct relevance to the question. The model does not appear to indicate the likelihood of the risk being realised. If the model is understood by all participants and is repeatable then it may help the design process
12.	Do you think the proposed risk model could help to identify risks?	Y / N / Not Sure	Y / N / Not Sure	Y / N / Not Sure	By having to model the risk it does encourage designers to think about risk but I believe the knowledge, method and tools used to establish the risk is what provides the real value.
13.	Do you think the proposed risk model could help the analysis of identified risks?	Y / N / Not Sure	Y / N / Not Sure	Y / N / Not Sure	If the risk model can be generated in a consistent manner and is repeatable then it would help facilitate automated analysis; however, experience of modelling security risks suggests this is very difficult.
14.	Do you think the proposed risk model could help with the assessment of analysed risks?	Y / N / Not Sure	Y / N / Not Sure	Y / N / Not Sure	Having modelled risks should enable the running of more analysis scenarios and therefore improve the assessment of analysed risk.
15.	Do you think the proposed risk model could help the mitigation of assessed risks?	Y / N / Not Sure	Y / N / Not Sure	Y / N / Not Sure	Where time has been taken to assess risk, it is likely that the output of the work will help to understand the mitigation options.

16.	Do you think the proposed risk model could help monitoring of ongoing risks?	Y / N / Not Sure	Y / N / Not Sure	Y / N / Not Sure	Much will depend on how easy it is to create and maintain the model accuracy
17.	Do you think the proposed risk model could be useful when a design model doesn't exist?	Y / N / Not Sure	Y / N / Not Sure	Y / N / Not Sure	
#	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?			Modelling the risk will allow the introduction of automated analysis tools If consistent, then a greater understanding of risks will be established within the design team and models can be re-used	
19.	Which approach (textural description or the proposed risk model) do you prefer and why?			Due to the complexities of risk, the cost of modelling and having models that can be understood by a range of users. I prefer risks to be described in textual descriptions. However, accurate risk models can be generated (as reasonable cost) then the ability to run automated analysis could be attractive.	
20.	Do you think any of the entities or associations in the proposed model are unnecessary or overkill, if so which ones?				
21.	Can you think of any entities or associations that are missing from the proposed risk model?			Likelihood	

Andrew Leigh, Michel Wermelinger, Andrea Zisman

22.	Do you have any other feedback about the proposed risk model or its usage?	
-----	--	--