

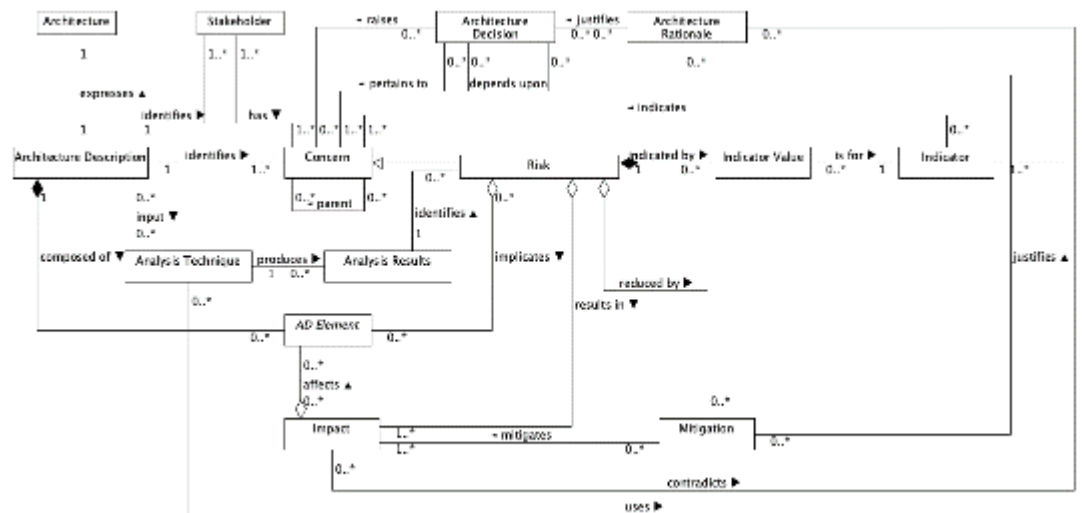
Architecture Risk Model Research Questionnaire

Section 1 – Participant Experience & Background

1. How many years of experience do you have in commercial software intensive systems engineering? **24 years**
2. How many years of experience do you have in commercial software development? **20 years**
3. How many years of enterprise architecture experience do you have? **4 years**
4. How many years of solution architecture experience do you have? **30 years**
5. How many years of technical architecture experience do you have? **30 years**
6. How many years of SysML experience do you have? **5 years**
7. How many years of UML experience do you have? **20 years**
8. How many projects have you worked on that have involved a SysML or UML model? **10 med/large Prjs**
9. How many years do you have working with waterfall development? **30 years**
10. How many years do you have working with agile (e.g. Scrum & SAE) development? **3 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

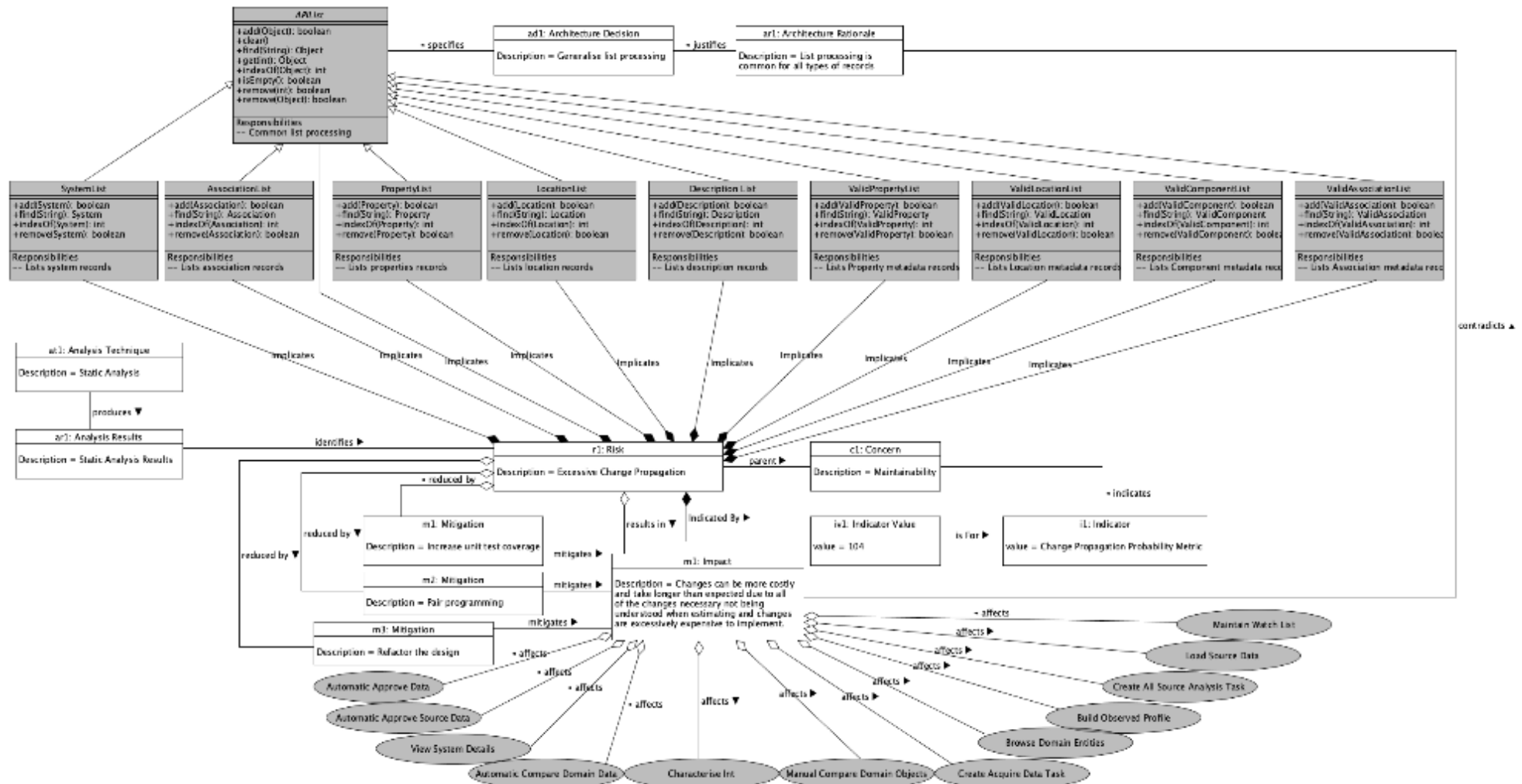
Text Risk Description

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.



Example 2 - 3rd Party Interface Changes outside of MASS control

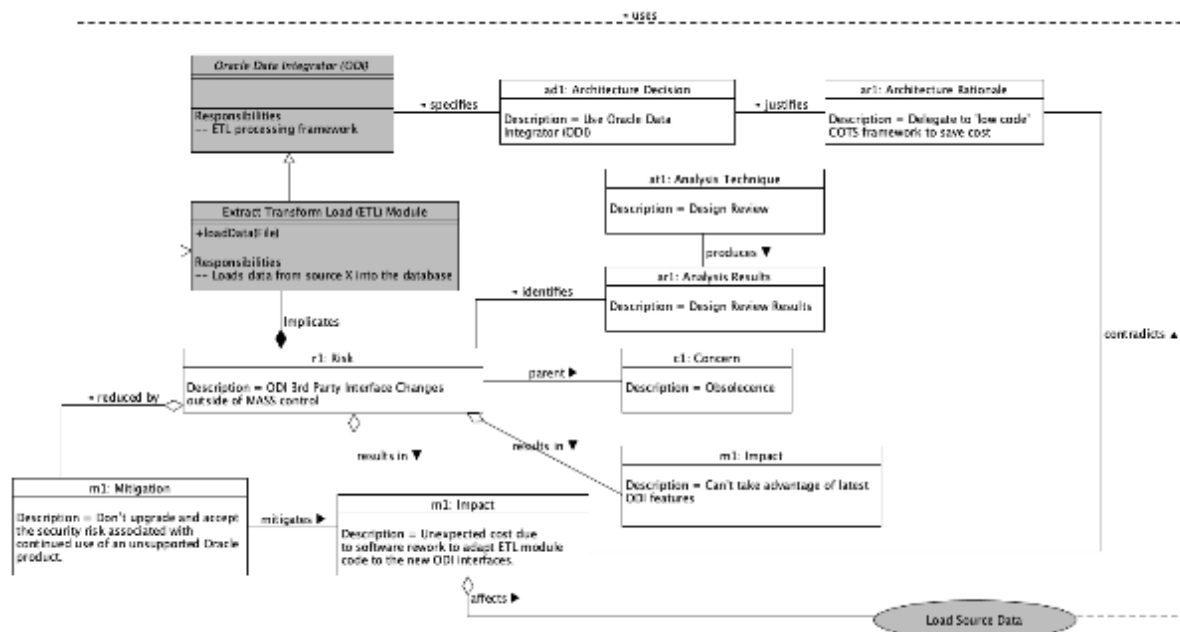
Text Risk Description

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. SAFe	
11.	Do you think the proposed risk model would help design reviews?	Y	Not Sure	Not Sure	Bringing a UML risk notation to design review would help explain design decision mitigations, clarify where the risk is within the design. However, it does clutter the design and therefore understanding of the design. Would have as a separate view/diagram of the design area. Would definitely help with waterfall as have clear architecture design/detailed design phases with reviews. Agile tends to be focused on short term design/delivery of a few requirements not big picture design risks. Example 1 is mixing software design with software process mitigations – again two views may help convey understanding.
12.	Do you think the proposed risk model could help to identify risks?	Not Sure	Not Sure	Not Sure	The model is a notation for describing risks/mitigations and what area of the design they apply to. Risks tend to be either obvious or identified through experience with previous projects not through having a notation. That said however, having a modelling notation and diagrammatic way of expressing risks would focus the engineer's thoughts and may assist in identifying design risk areas.
13.	Do you think the proposed risk model could help the analysis of identified risks?	Y	Y	Y	Having a diagrammatic way of expressing risk, mitigation and identifying them against classes, areas of functionality would help with analysis and eliciting different design pattern options to mitigate identified risk areas.
14.	Do you think the proposed risk model could help with the assessment of analysed risks?	Y	Y	Y	Again having a picture to talk around with team members and wider stakeholders would help with the assessment as opposed to a plain tabular list.
15.	Do you think the proposed risk model could help the mitigation of assessed risks?	Not Sure	Not Sure	Not Sure	Having a modelling notation is different from a methodology, being able to express a mitigation doesn't necessarily make it a good one. That said having a team being able to discuss mitigation options round a picture would definitely help

					creatively.
16.	Do you think the proposed risk model could help monitoring of ongoing risks?	Y	Y	Y	Having the risks on the working design UML would help keep them in focus in the engineers mind as opposed to being tucked away in a separate log and only brought out by the PM at big reviews.
17.	Do you think the proposed risk model could be useful when a design model doesn't exist?	Y	Y	Y	Very often risks are very top level spanning the project, having them documented and visual prior to starting the design would help influence the design to mitigate the risks. Being able to attach risks to user stories/requirements during the requirement analysis phase would be helpful in communicating risk to the implementation team.
#	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?	Having a diagrammatic notation to visualise risk, mitigations and associate them against requirements, classes, aspects of the design would help communicate them inside and outside the team. Concerns over cluttering UML diagrams would over complicate them, losing design clarity, having them as separate views would help.			
19.	Which approach (textural description or the proposed risk model) do you prefer and why?	I think and see software/system architecture better visually. Having risk/mitigations in the same UML design tool would help focus on these aspects during design than having a separate list I had to refer to maintain. Also, as I go through my design as risks occur they could easily be put on the diagram as the same time.			
20.	Do you think any of the entities or associations in the proposed model are unnecessary or overkill, if so which ones?	I think architecture rationale would be better being an attribute of architecture decision as opposed to being a separate class.			
21.	Can you think of any entities or associations that are missing from the proposed risk model?	Good to have a way of expressing probability and expressing impact level – high, medium, low. Could use colour coding on class boxes? And attributes/properties of Impact classes.			

Andrew Leigh, Michel Wermelinger, Andrea Zisman

22.	Do you have any other feedback about the proposed risk model or its usage?	Could set up some stereotypes in System Architect and apply it to different types of project/size.