

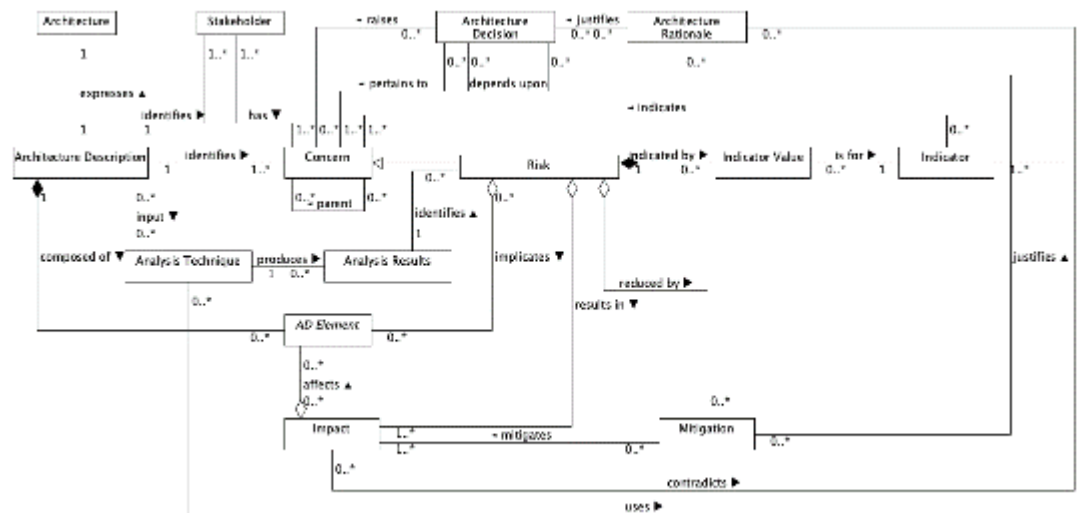
Architecture Risk Model Research Questionnaire

Section 1 – Participant Experience & Background

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

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

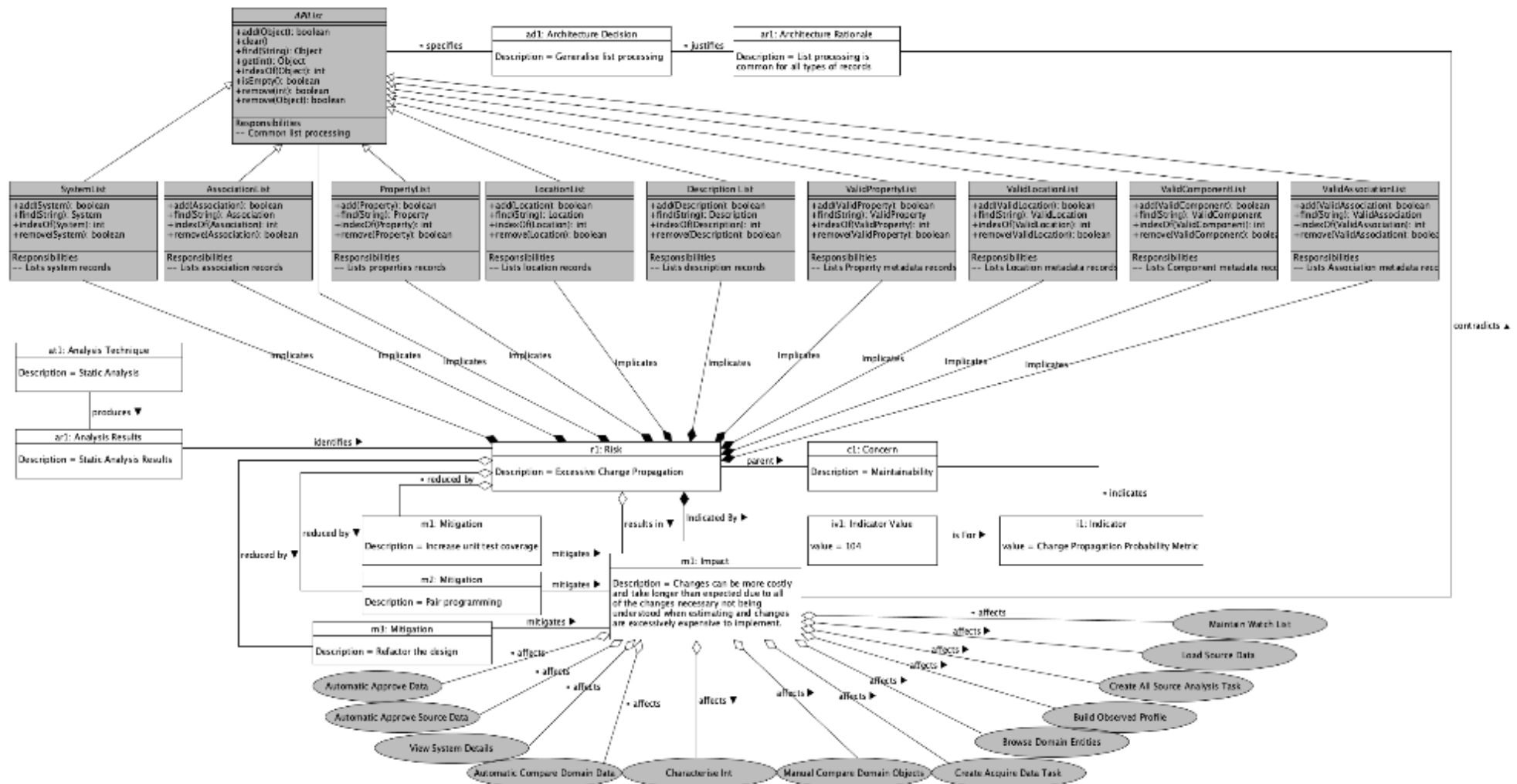
Title:	Excessive change propagation
Details:	Complex concrete sub-classes have emerged from the diverse use cases the lists had to support. E.g. SystemList needs “deleted record processing” whereas PropertyList does not. This causes conflicts between abstract class code and concrete sub-class code. This 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:

The three mitigation

- 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.

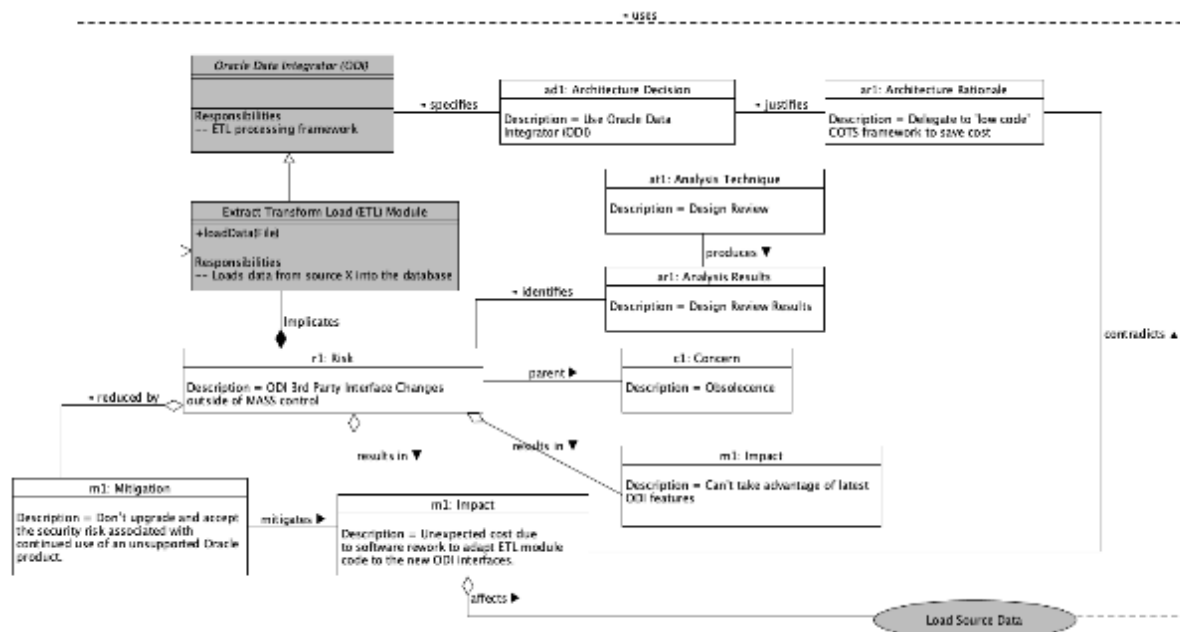
Impact: Unexpected cost due to software rework to adapt ETL module code to the new ODI interfaces. Can't take advantage of latest ODI features.

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	<p>I'm not sure I'm experienced enough to see many models that include the model of 'what it is' as well as 'how it's built'.</p> <p>Putting the how and why further into the <i>formal</i> class model (rather than into whiteboards, JIRA instances, Jupyter Notebooks, Slack rooms, Confluence pages etc) might create a bigger overhead than it's worth to deal with technical debt.</p>
12.	Do you think the proposed risk model could help to identify risks?	Y	Y	Y	<p>I find it to be able to 'value' a risk without the impact relating to a stakeholder concern.</p> <p>All your examples are risks in relation to <i>building</i> the architecture, not in using the system the architecture describes. Is this the explicit limit of the model?</p> <p>It appears that the risks are at the project level - of bringing the system of interest into being or managing it afterwards?</p> <p>Is the aim really to manage technical debt (really a risk or a technical insurance premium?) https://www.linkedin.com/pulse/thoughts-technical-debt-graham-berrisford/?published=t</p>
13.	Do you think the proposed risk model could help the analysis of identified risks?	Not Sure	Not Sure	Not Sure	<p>Again, the fact that the risk is formally associated with the architecture is good. But most of the analysis will be done during, the time that well, the analysis technique is applied.</p>
14.	Do you think the proposed risk model could help with the assessment of analysed	Not Sure	Not Sure	Not Sure	<p>Not sure, but probably not. Again, formally connecting the risk management up to the architecture is good. But the whole practice of risk management is larger, with different cycles and</p>

	risks?				granularity at different stages for this to be useful.
Eful. 15.	Do you think the proposed risk model could help the mitigation of assessed risks?	Not Sure	Not Sure	Not Sure	Risk mitigation in some models includes things that don't really reduce a risk at all https://www.glynholton.com/blog/risk-management/4-ts-overlook/ . Often managing a risk is more than just reducing it. But the language in the descriptions below mean that the 'Risk' is 'reduced by' seems very similar to Impact is 'mitigated by' (I know I've reversed the direction). The number of options in reality, the number of iterations might make this unworkable visually.
16.	Do you think the proposed risk model could help monitoring of ongoing risks?	N	N	N	The design is likely to get lost in the building plans. Mixing visually the design with the plans at the UML level is challenging. Maybe while the examples use UML, the ADL is really at the content for the Architecture Description, and that 'document' could just as well be the issue repository like JIRA, that would work.
17.	Do you think the proposed risk model could be useful when a design model doesn't exist?	Not Sure	Not Sure	Not Sure	The first example is a code quality issue, the second one is a dependency issue. I can't see where
#	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?			I think it will get overwhelming quickly. I can't see how	
19.	Which approach (textural description or the proposed risk model) do you prefer and why?			I think the choice isn't mutually exclusive. I'd rather see a framework for actively managing risks that are formally connected to the solution.	

20.	Do you think any of the entities or associations in the proposed model are unnecessary or overkill, if so which ones?	<p>The analysis technique seems overkill. I'm not sure how this is that useful in the examples below. Unless they are relevant for how the risk might be mitigated (especially if it's not <i>just</i> reducing the impact). The 'impact results' seems undercooked.</p> <p>Also, in the first example, the 'impact affects' elements gave no real help.</p>
21.	Can you think of any entities or associations that are missing from the proposed risk model?	At the risk of making it even more complex, I would like to have seen probability addressed directly.
22.	Do you have any other feedback about the proposed risk model or its usage?	An artefact of the English language is that things like 'mitigation mitigates' feel a little underwhelming. 'Indicates the relative risk of a Risk ' is circular. You've used a term 'untreated' in the definition that's quite specific to risk management, but that term not used in the associations.