USC

USC Viterbi
School of Engineering

Architecture-Based Software Reliability Estimation: Problem Space, Challenges and Strategies

Ivo Krka

Leslie Cheung

George Edwards

Leana Golubchik

Nenad Medvidovic

Motivation

- Early non-functional analysis more cost effective

- Current techniques oversimplify numerous factors
  - Definition of system’s reliability – “reliability is the probability of failure-free operation for a specified time in a specified environment” – is not complete
  - Parameters influencing system’s reliability
    - → Larger number than assumed
    - → Greater complexity
    - → Lacking classification of parameter space in the literature
  - Information sources
    - → Parameter values rarely readily available, precise, and complete

Problem Space

- Reliability is a complex property
  - Different meanings, characteristics, and associated metrics in different contexts
- How do we define failure for an arbitrary software system?
  - System is considered failed if some of its components fail?
  - The real definition is more specific and depends on the requirements on the system
- Different failures – different weights
- Different usage models and stakeholders – different failure definitions
- Computational environment is very complex

Reliability Ingredients

Reliability ingredient		Instantiation
Failure information	Failure-free behavior definition	
	Failure severity	critical vs. minor
	Failure impact	system-wide vs. local
	Failure extent	complete vs. partial
	Probability of failure	
Operational profile	Service execution frequency	
	User inputs	user inputs frequencies
	Operational contexts	
Recovery information	Likelihood of recovery	
	Time to recovery	
	Recovery mechanism	redundancy, replication
	Recovery process	redeployment
	Extent of recovery	

Reliability Ingredients

Reliability ingredient		Instantiation
Failure information	Failure-free behavior definition	
	Failure severity	critical vs. minor
	Failure impact	system-wide vs. local
	Failure extent	complete vs. partial
	Probability of failure	
Operational profile	Service execution frequency	
	User inputs	user inputs frequencies
	Operational contexts	
Recovery information	Likelihood of recovery	
	Time to recovery	
	Recovery mechanism	redundancy, replication
	Recovery process	redeployment
	Extent of recovery	

Reliability Ingredients

Reliability ingredient		Instantiation
Failure information	Failure-free behavior definition	
	Failure severity	critical vs. minor
	Failure impact	system-wide vs. local
	Failure extent	complete vs. partial
	Probability of failure	
Operational profile	Service execution frequency	
	User inputs	user inputs frequencies
	Operational contexts	
Recovery information	Likelihood of recovery	
	Time to recovery	
	Recovery mechanism	redundancy, replication
	Recovery process	redeployment
	Extent of recovery	

Reliability Ingredients

Reliability ingredient		Instantiation
Failure information	Failure-free behavior definition	
	Failure severity	critical vs. minor
	Failure impact	system-wide vs. local
	Failure extent	complete vs. partial
	Probability of failure	
Operational profile	Service execution frequency	
	User inputs	user inputs frequencies
	Operational contexts	
Recovery information	Likelihood of recovery	
	Time to recovery	
	Recovery mechanism	redundancy, replication
	Recovery process	redeployment
	Extent of recovery	

Reliability Ingredients

Reliability ingredient		Instantiation
Failure information	Failure-free behavior definition	
	Failure severity	critical vs. minor
	Failure impact	system-wide vs. local
	Failure extent	complete vs. partial
	Probability of failure	
Operational profile	Service execution frequency	
	User inputs	user inputs frequencies
	Operational contexts	
Recovery information	Likelihood of recovery	
	Time to recovery	
	Recovery mechanism	redundancy, replication
	Recovery process	redeployment
	Extent of recovery	

Reliability Ingredients

Reliability ingredient		Instantiation
Failure information	Failure-free behavior definition	
	Failure severity	critical vs. minor
	Failure impact	system-wide vs. local
	Failure extent	complete vs. partial
	Probability of failure	
Operational profile	Service execution frequency	
	User inputs	user inputs frequencies
	Operational contexts	
Recovery information	Likelihood of recovery	
	Time to recovery	
	Recovery mechanism	redundancy, replication
	Recovery process	redeployment
	Extent of recovery	

Reliability Ingredients

Reliability ingredient		Instantiation
Failure information	Failure-free behavior definition	
	Failure severity	critical vs. minor
	Failure impact	system-wide vs. local
	Failure extent	complete vs. partial
	Probability of failure	
Operational profile	Service execution frequency	
	User inputs	user inputs frequencies
	Operational contexts	
Recovery information	Likelihood of recovery	
	Time to recovery	
	Recovery mechanism	redundancy, replication
	Recovery process	redeployment
	Extent of recovery	

Reliability Ingredients

Reliability ingredient		Instantiation
Failure information	Failure-free behavior definition	
	Failure severity	critical vs. minor
	Failure impact	system-wide vs. local
	Failure extent	complete vs. partial
	Probability of failure	
Operational profile	Service execution frequency	
	User inputs	user inputs frequencies
	Operational contexts	
Recovery information	Likelihood of recovery	
	Time to recovery	
	Recovery mechanism	redundancy, replication
	Recovery process	redeployment
	Extent of recovery	

Reliability Ingredients

Reliability ingredient		Instantiation
Failure information	Failure-free behavior definition	
	Failure severity	critical vs. minor
	Failure impact	system-wide vs. local
	Failure extent	complete vs. partial
	Probability of failure	
Operational profile	Service execution frequency	
	User inputs	user inputs frequencies
	Operational contexts	
Recovery information	Likelihood of recovery	
	Time to recovery	
	Recovery mechanism	redundancy, replication
	Recovery process	redeployment
	Extent of recovery	

Reliability Ingredients

Reliability ingredient		Instantiation
Failure information	Failure-free behavior definition	
	Failure severity	critical vs. minor
	Failure impact	system-wide vs. local
	Failure extent	complete vs. partial
	Probability of failure	
Operational profile	Service execution frequency	
	User inputs	user inputs frequencies
	Operational contexts	
Recovery information	Likelihood of recovery	
	Time to recovery	
	Recovery mechanism	redundancy, replication
	Recovery process	redeployment
	Extent of recovery	

Reliability Ingredients

Reliability ingredient		Instantiation
Failure information	Failure-free behavior definition	
	Failure severity	critical vs. minor
	Failure impact	system-wide vs. local
	Failure extent	complete vs. partial
	Probability of failure	
Operational profile	Service execution frequency	
	User inputs	user inputs frequencies
	Operational contexts	
Recovery information	Likelihood of recovery	
	Time to recovery	
	Recovery mechanism	redundancy, replication
	Recovery process	redeployment
	Extent of recovery	

Reliability Ingredients

Reliability ingredient		Instantiation
Failure information	Failure-free behavior definition	
	Failure severity	critical vs. minor
	Failure impact	system-wide vs. local
	Failure extent	complete vs. partial
	Probability of failure	
Operational profile	Service execution frequency	
	User inputs	user inputs frequencies
	Operational contexts	
Recovery information	Likelihood of recovery	
	Time to recovery	
	Recovery mechanism	redundancy, replication
	Recovery process	redeployment
	Extent of recovery	

Reliability Ingredients

Reliability ingredient		Instantiation
Failure information	Failure-free behavior definition	
	Failure severity	critical vs. minor
	Failure impact	system-wide vs. local
	Failure extent	complete vs. partial
	Probability of failure	
Operational profile	Service execution frequency	
	User inputs	user inputs frequencies
	Operational contexts	
Recovery information	Likelihood of recovery	
	Time to recovery	
	Recovery mechanism	redundancy, replication
	Recovery process	redeployment
	Extent of recovery	

Reliability Ingredients

Reliability ingredient		Instantiation
Failure information	Failure-free behavior definition	
	Failure severity	critical vs. minor
	Failure impact	system-wide vs. local
	Failure extent	complete vs. partial
	Probability of failure	
Operational profile	Service execution frequency	
	User inputs	user inputs frequencies
	Operational contexts	
Recovery information	Likelihood of recovery	
	Time to recovery	
	Recovery mechanism	redundancy, replication
	Recovery process	redeployment
	Extent of recovery	

Reliability Ingredients

Reliability ingredient		Instantiation	Example of architecture as an information source
Failure information	Failure-free behavior definition		specification of intended behavior
	Failure severity	critical vs. minor	specification of criticality of service
	Failure impact	system-wide vs. local	interaction and deployment specification
	Failure extent	complete vs. partial	specification of user's interactions
	Probability of failure		not applicable
Operational profile	Service execution frequency		not applicable
	User inputs	user inputs frequencies	inputs specification (frequencies not available)
	Operational contexts		specifications of behaviors, concurrency mechanisms, computational resources
Recovery information	Likelihood of recovery		not applicable
	Time to recovery		not available
	Recovery mechanism	redundancy, replication	specification of recovery enabling operations during normal system operation
	Recovery process	redeployment	specification of steps taken to recover from a failure
	Extent of recovery		partially available

Reliability Ingredients

Reliability ingredient		Instantiation	Example of architecture as an information source
Failure information	Failure-free behavior definition		specification of intended behavior
	Failure severity	critical vs. minor	specification of criticality of service
	Failure impact	system-wide vs. local	interaction and deployment specification
	Failure extent	complete vs. partial	specification of user's interactions
	Probability of failure		not applicable
Operational profile	Service execution frequency		not applicable
	User inputs	user inputs frequencies	inputs specification (frequencies not available)
	Operational contexts		specifications of behaviors, concurrency mechanisms, computational resources
Recovery information	Likelihood of recovery		not applicable
	Time to recovery		not available
	Recovery mechanism	redundancy, replication	specification of recovery enabling operations during normal system operation
	Recovery process	redeployment	specification of steps taken to recover from a failure
	Extent of recovery		partially available

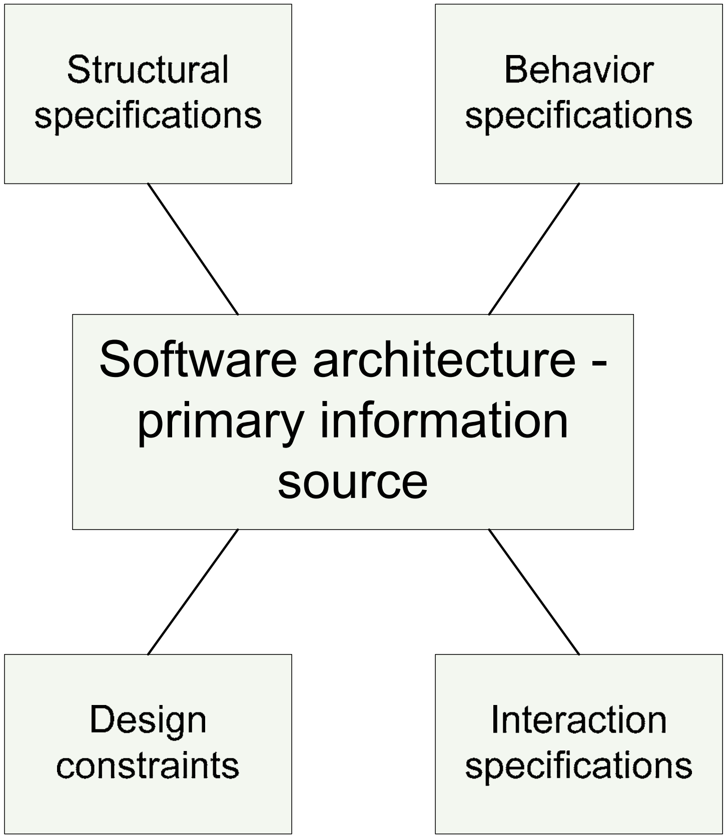
Reliability Ingredients

Reliability ingredient		Instantiation	Example of architecture as an information source
Failure information	Failure-free behavior definition		specification of intended behavior
	Failure severity	critical vs. minor	specification of criticality of service
	Failure impact	system-wide vs. local	interaction and deployment specification
	Failure extent	complete vs. partial	specification of user's interactions
	Probability of failure		not applicable
Operational profile	Service execution frequency		not applicable
	User inputs	user inputs frequencies	inputs specification (frequencies not available)
	Operational contexts		specifications of behaviors, concurrency mechanisms, computational resources
Recovery information	Likelihood of recovery		not applicable
	Time to recovery		not available
	Recovery mechanism	redundancy, replication	specification of recovery enabling operations during normal system operation
	Recovery process	redeployment	specification of steps taken to recover from a failure
	Extent of recovery		partially available

Available Information Sources

Software architecture - primary information source

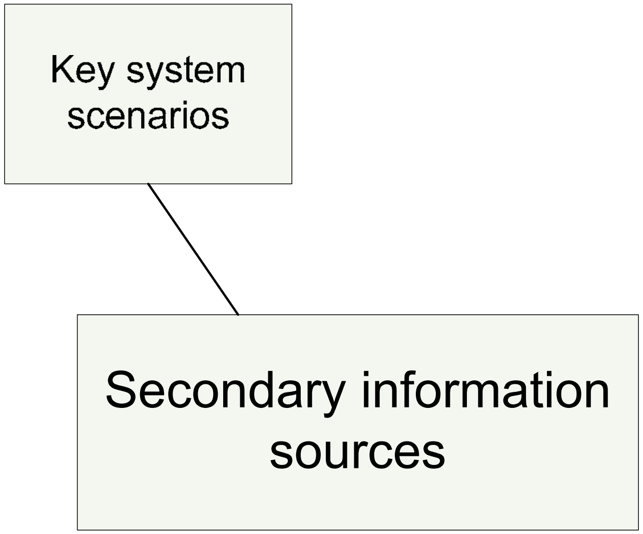
Available Information Sources


Structural specifications
Behavior specifications
Software architecture - primary information source
Design constraints
Interaction specifications

Available Information Sources

Secondary information sources

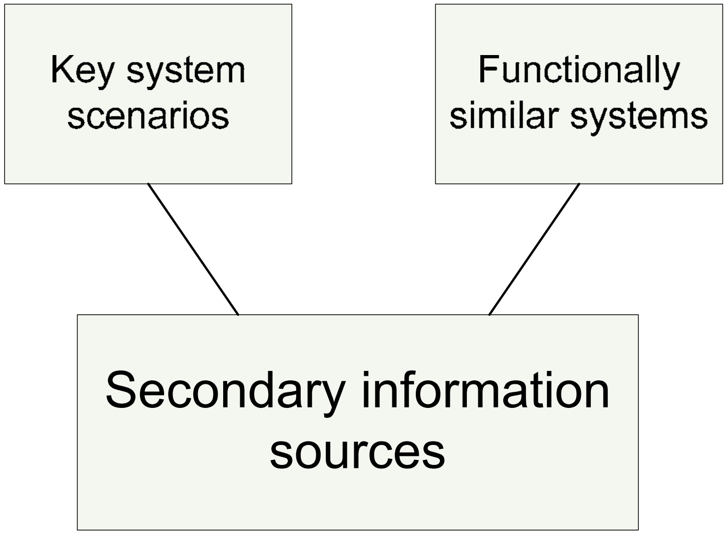
Available Information Sources



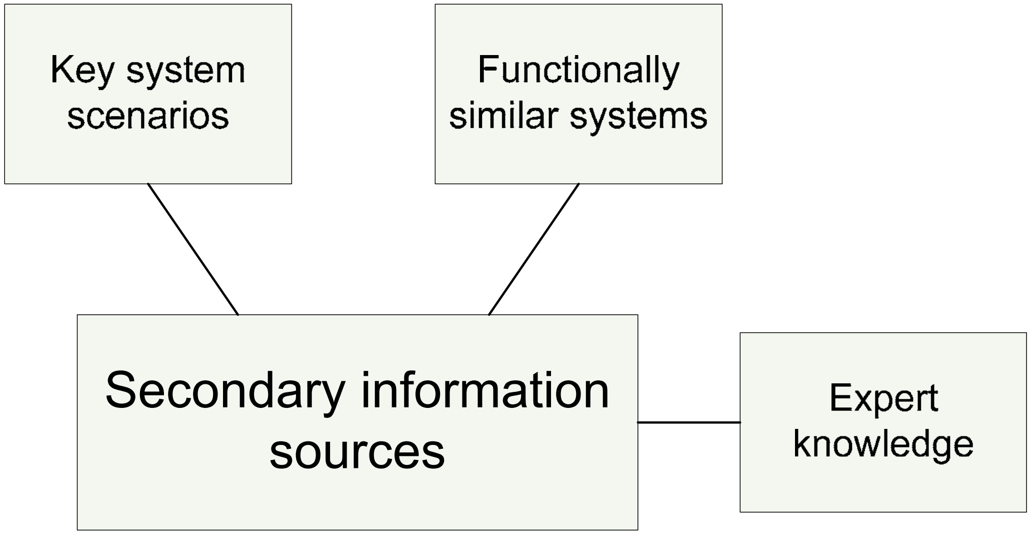
Key system scenarios

Secondary information sources

Available Information Sources



Available Information Sources



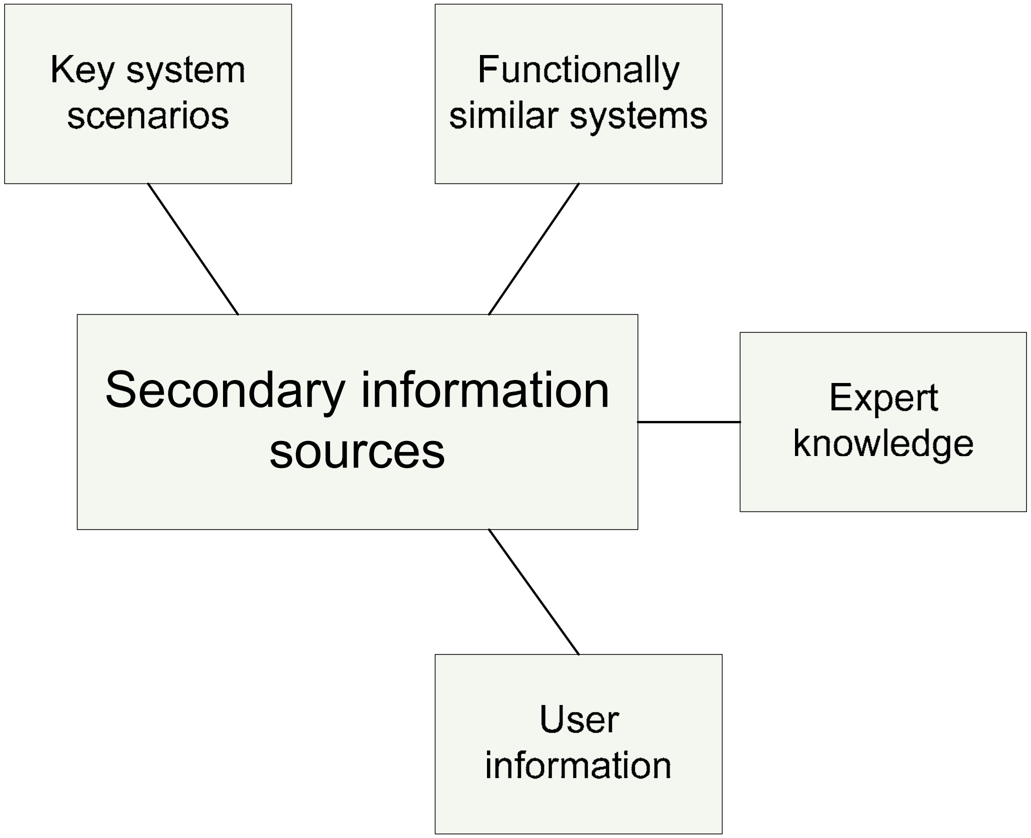
Key system scenarios

Functionally similar systems

Secondary information sources

Expert knowledge

Available Information Sources



Key system scenarios

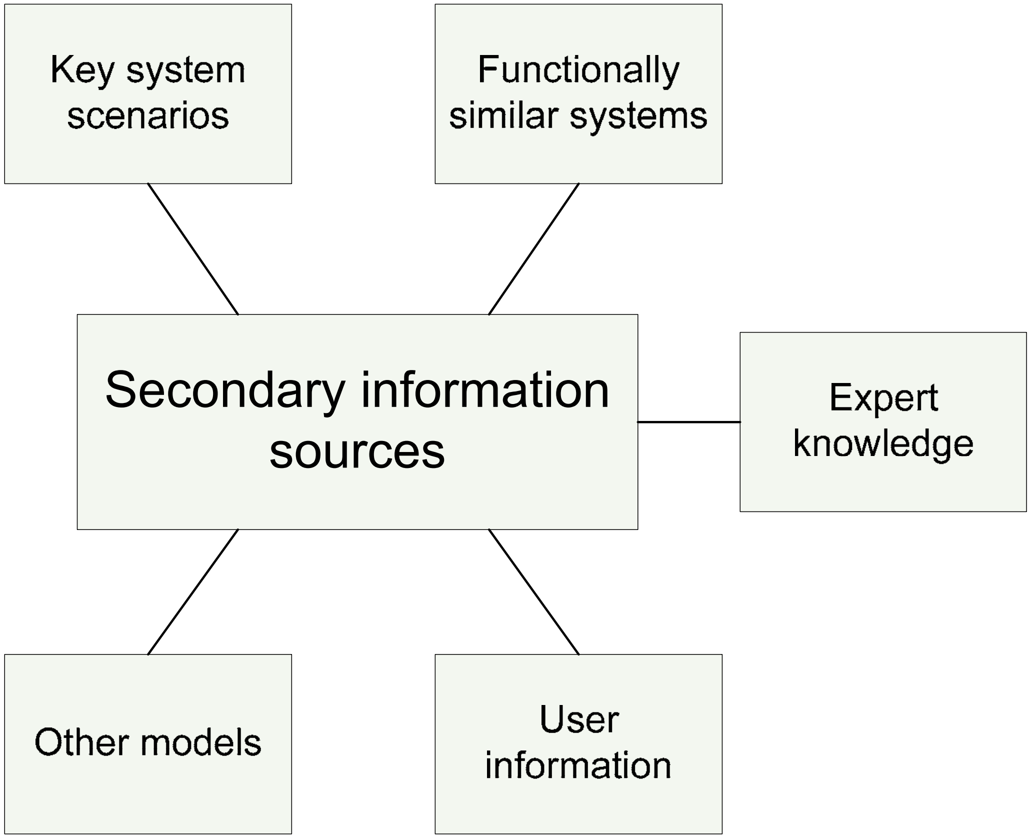
Functionally similar systems

Secondary information sources

Expert knowledge

User information

Available Information Sources



Secondary information sources

Key system scenarios

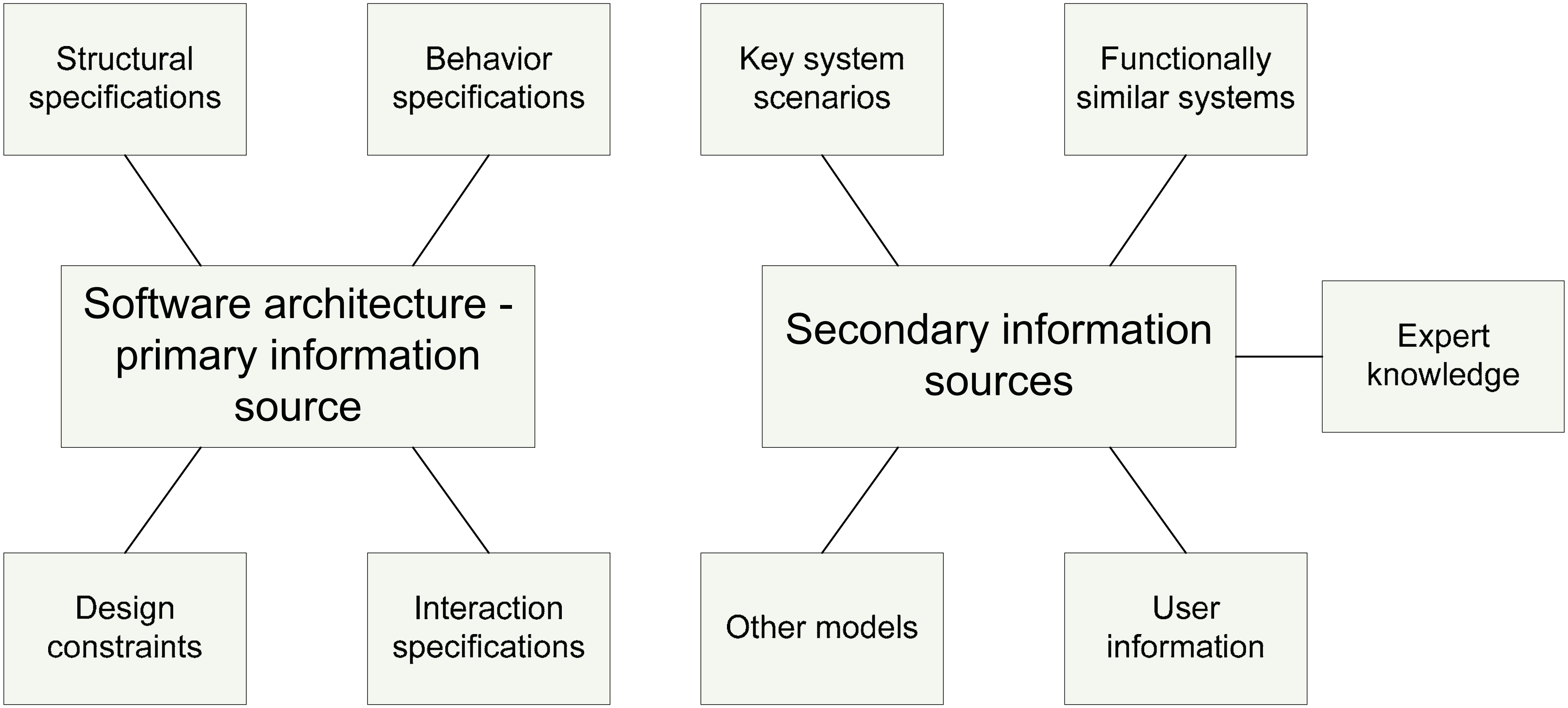
Functionally similar systems

Expert knowledge

Other models

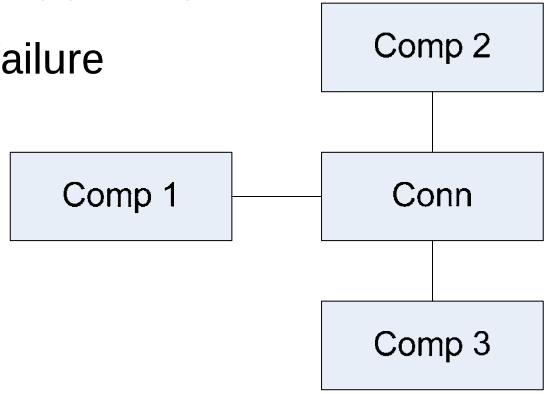
User information

Available Information Sources


Structural specifications
Behavior specifications
Key system scenarios
Functionally similar systems
Software architecture - primary information source
Secondary information sources
Expert knowledge
Design constraints
Interaction specifications
Other models
User information

Current Strategies in Light of Reliability Ingredients

1. Every approach has some kind of failure-free operation definition
   - Failure of any particular component/service is a system failure
   - Boolean combination of individual component failures (e.g., $(C1.F \wedge C3.F) \vee C2.F$) is a system failure



2. Some approaches can consider failure severity
   - Cheung et al., Goseva-Popstojanova et al.
   - Multiple failure states account for different failure severities

3. Most approaches ignore failure impact
   - Cortellessa et al. allow an architect to specify a probability of propagation

4. All approaches do not differentiate between failure extents

Current Strategies in Light of Reliability Ingredients

5. Failure probabilities are used in analysis
   - Only some approaches explore their derivation
     - → Cheung et al. use architectural defect classification to derive possible failures
     - → Goseva-Popstojanova et al. use a complexity metric
     - → Reussner et al. derive failure probability from reliabilities of method bodies, calls, returns and environment

6. Frequencies of service executions used with different granularities
   - Probabilities of transitions between internal states, transfer of control between components, probabilities of execution of particular paths, etc.
   - Derivation of information explored only in Cheung et al.

7. User inputs mostly not considered
   - Cortellessa et al. use annotations on UML Use Case diagrams
     - → Derivation not explored

Current Strategies in Light of Reliability Ingredients

8. Little or no attention to the operational context
   - E.g., concurrency is either not considered or considered in a very limited manner

9. Most approaches do not consider likelihood of recovery

10. Most approaches do not consider time to recovery
    - Cheung et al. explicitly models likelihood of and time to recovery

11. Recovery mechanisms consideration not incorporated

12. Recovery process consideration not incorporated

13. Recovery extent consideration not incorporated

Conclusion and Future Work

- Contributions
  - Clear statement of the problem space
  - Comprehensive enumeration of reliability ingredients
  - Consideration of possible information sources
  - Critical overview of existing approaches

- Future Work
  - Tools allowing an architect analysis of reliability as a multi-faceted problem

    → Techniques that include a larger subset or reliability ingredients

    → Models for combining information from different sources
  - Techniques resolving additional shortcomings of existing approaches

    → Scalability problems