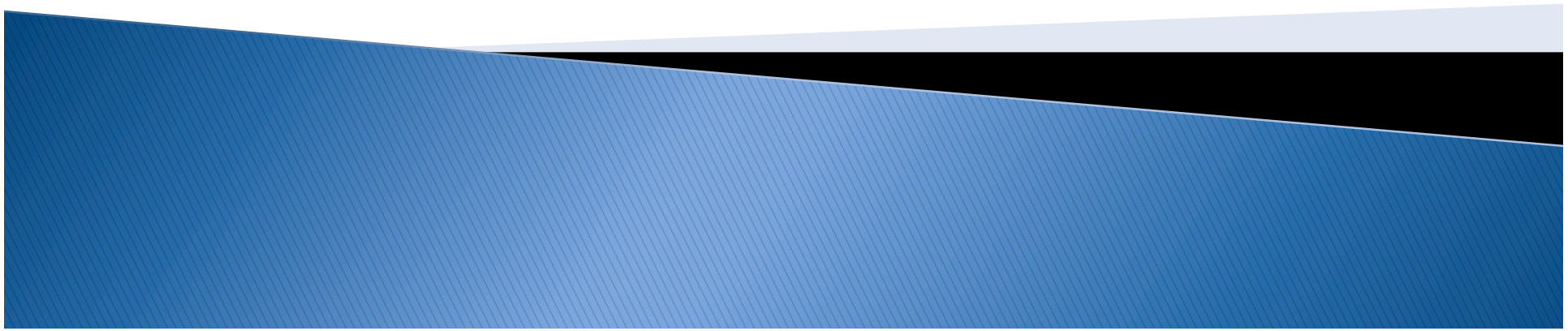
Research Report: A Take on Component-Based Software Systems' Reliability

Thanh-Trung Pham,
Xavier Défago, Quyet-Thang Huynh

School of Information Science,
Japan Advanced Institute of Science and Technology (JAIST)



Context / Activities

- Protocol Composition
  - Protocol Design
  - Verifiable Composition

- Component Reliability
  - Modeling
  - Prediction
  - Profiling

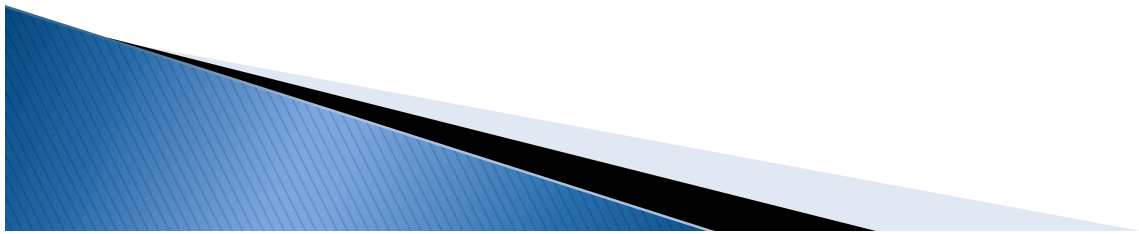
- Robot FT protocols / algorithms

Existing reliability prediction

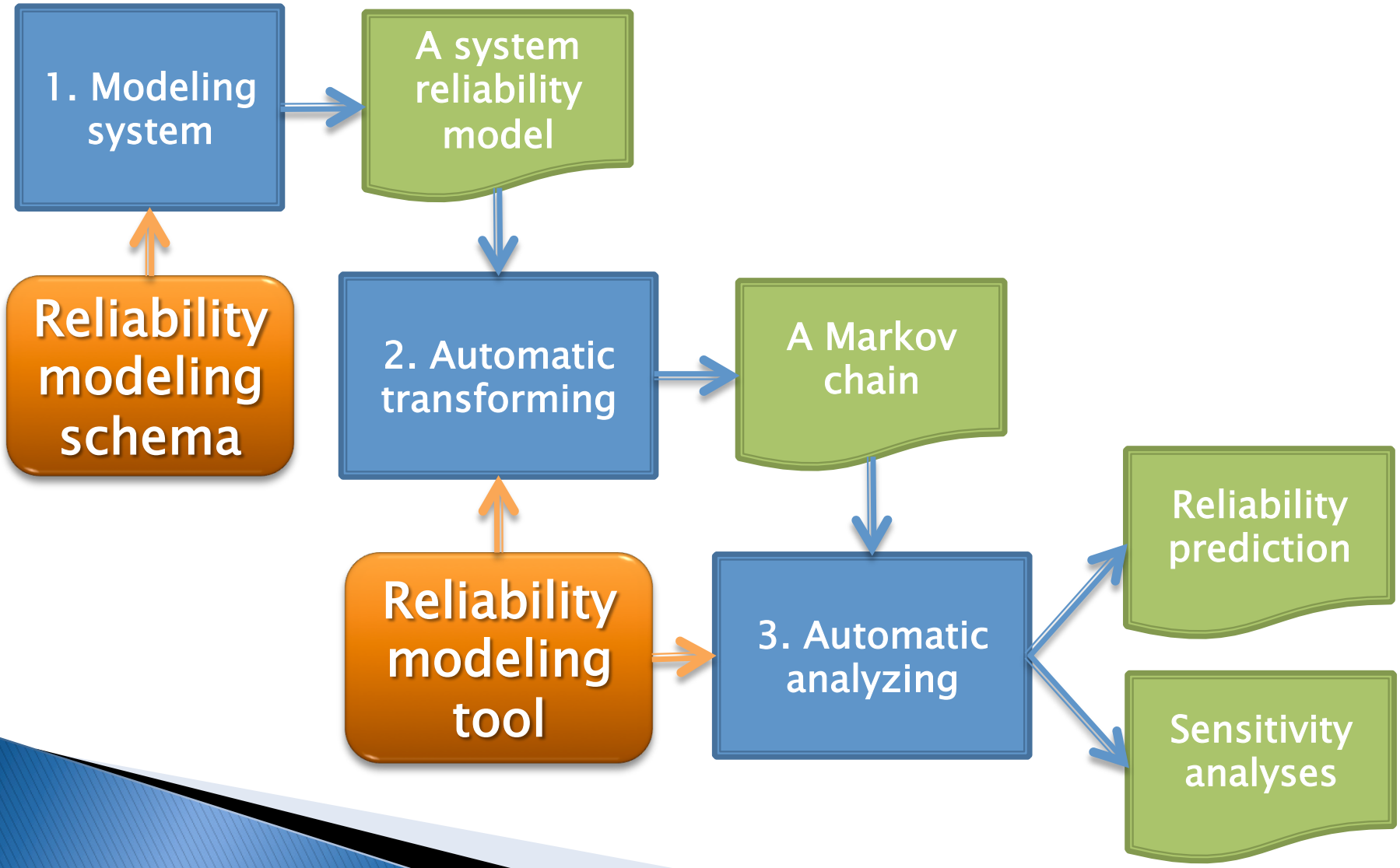
- Usually assume that [Immonen et al., 2008]:
  - Sequential execution model
    - At any instance of time, only one component is executing.
  - Stopping failure model
    - Components fail independently
    - a component failure leads to a total system failure.
- **Cannot model error propagation and concurrent/fault-tolerance executions**

Parts

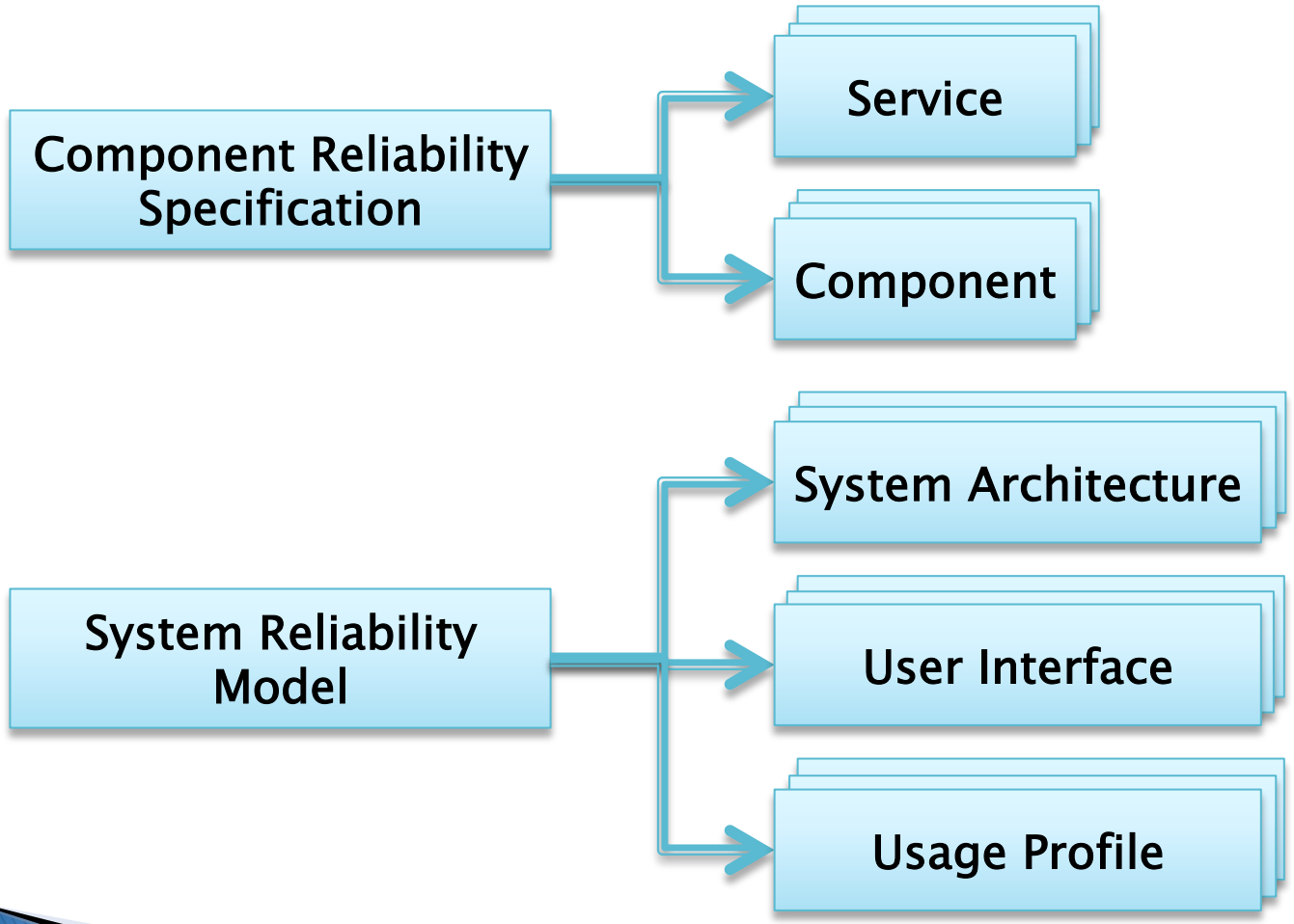
- Model
  - FT mechanisms
  - Error Propagation
- Tool
  - Automatic transformation / analysis
- Analysis
  - Sensitivity -> find reliability bottlenecks
  - Prediction -> specification assessment
- Validation
  - Using model / tool on actual software
  - Fault-injection



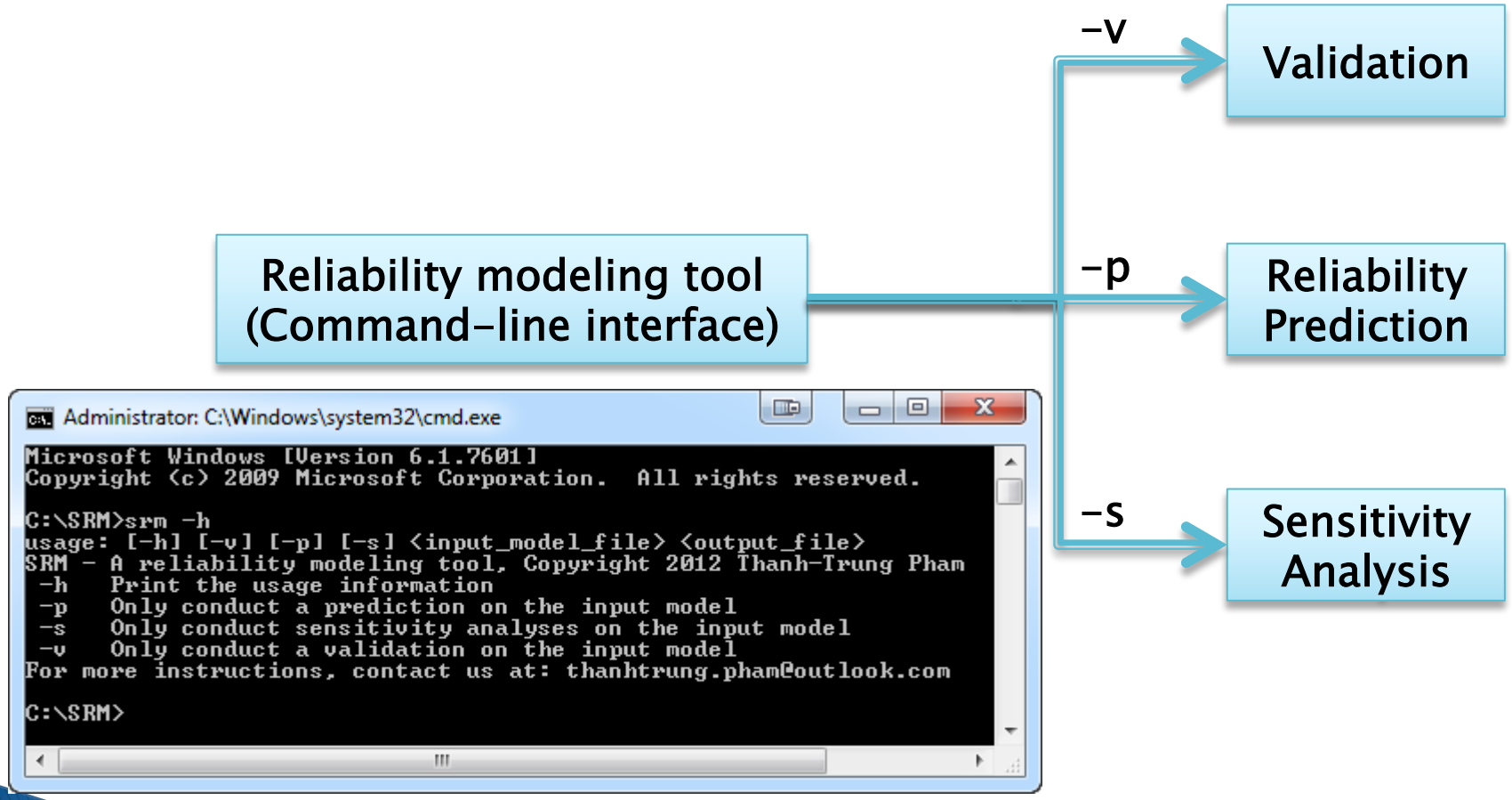
Component-based Reliability Prediction



Reliability Modeling Schema



Reliability Modeling Tool



A Sample of System Reliability Model

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:SystemReliabilityModeling xsi:schemaLocation="jaist.ac.jp SystemReliabilityModeling.xsd" xmlns:xsi="
http://www.w3.org/2001/XMLSchema-instance" xmlns:tns="jaist.ac.jp">
    <tns:ComponentReliabilitySpecification>
        <tns:Service name="processReportRequest"/>
        <tns:Service name="generateReport"/>
        <tns:Service name="viewRecentReports"/>
        <tns:Service name="getAttachmentDocumentInfo"/>
        <tns:Service name="getFileDocumentInfo"/>
        <tns:Service name="getReleasedDocumentInfoFromLogs"/>
        <tns:Service name="getReleasedDocumentInfoFromDB"/>
        <tns:Component name="SourceManager">
            <tns:ProvidedService forService="getAttachmentDocumentInfo"/>
            <tns:ProvidedService forService="getFileDocumentInfo"/>
            <tns:ServiceImplementation forService="getAttachmentDocumentInfo">
            <tns:ServiceImplementation forService="getFileDocumentInfo">
        </tns:Component>
        <tns:Component name="DestinationManager">
        <tns:Component name="Reporter">
        <tns:Component name="Mediator">
    </tns:ComponentReliabilitySpecification>
    <tns:SystemReliabilityModel>
        <tns:SystemArchitecture name="reportingServiceSystemArchitecture">
        <tns:UserInterface name="reportingServiceUserInterface" forSystemArchitecture="reportingServiceSystemArchitecture">
        <tns:UsageProfile forUserInterface="reportingServiceUserInterface">
    </tns:SystemReliabilityModel>
</tns:SystemReliabilityModeling>
```

Services

Components

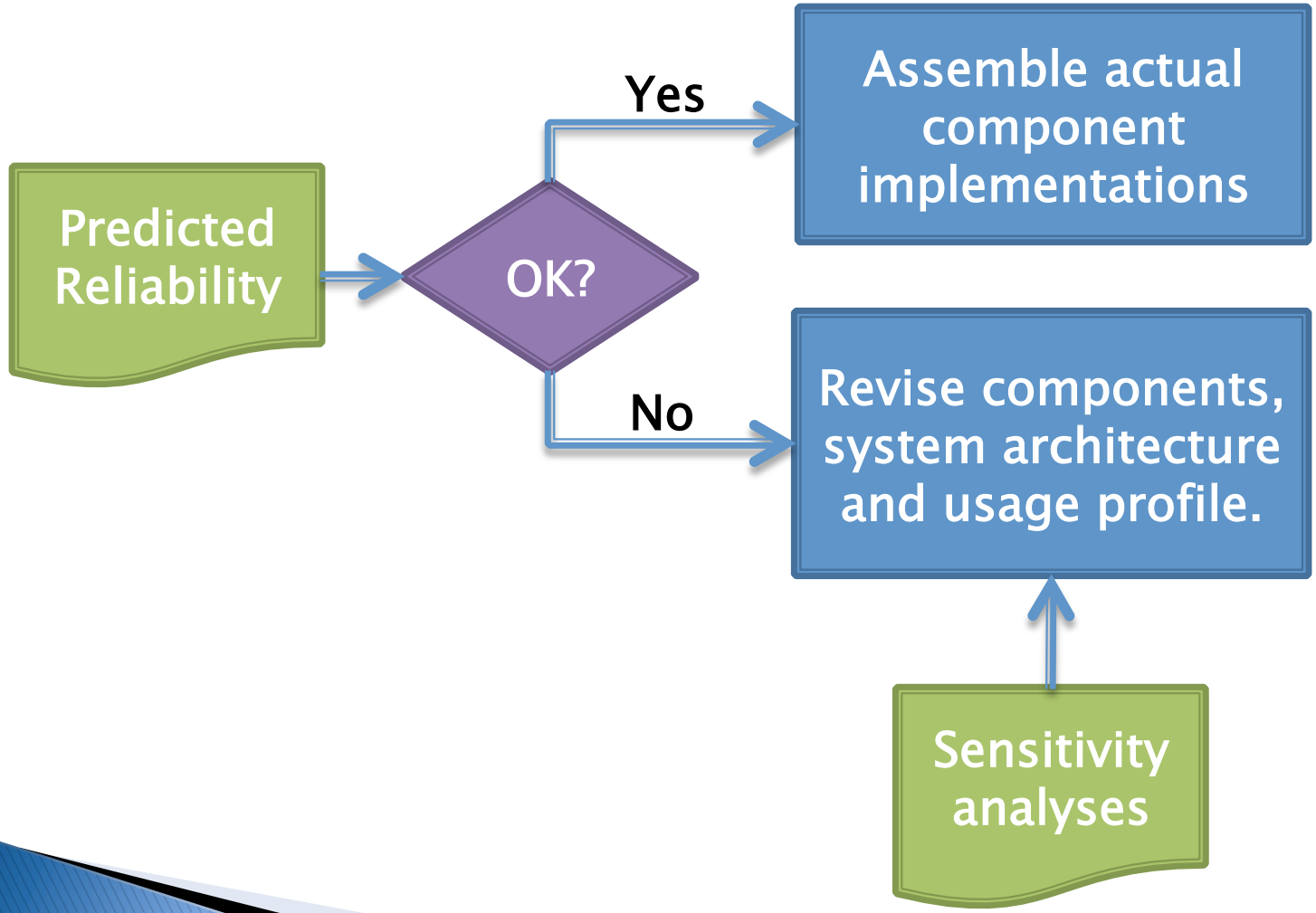
Service Implementations

System Architecture

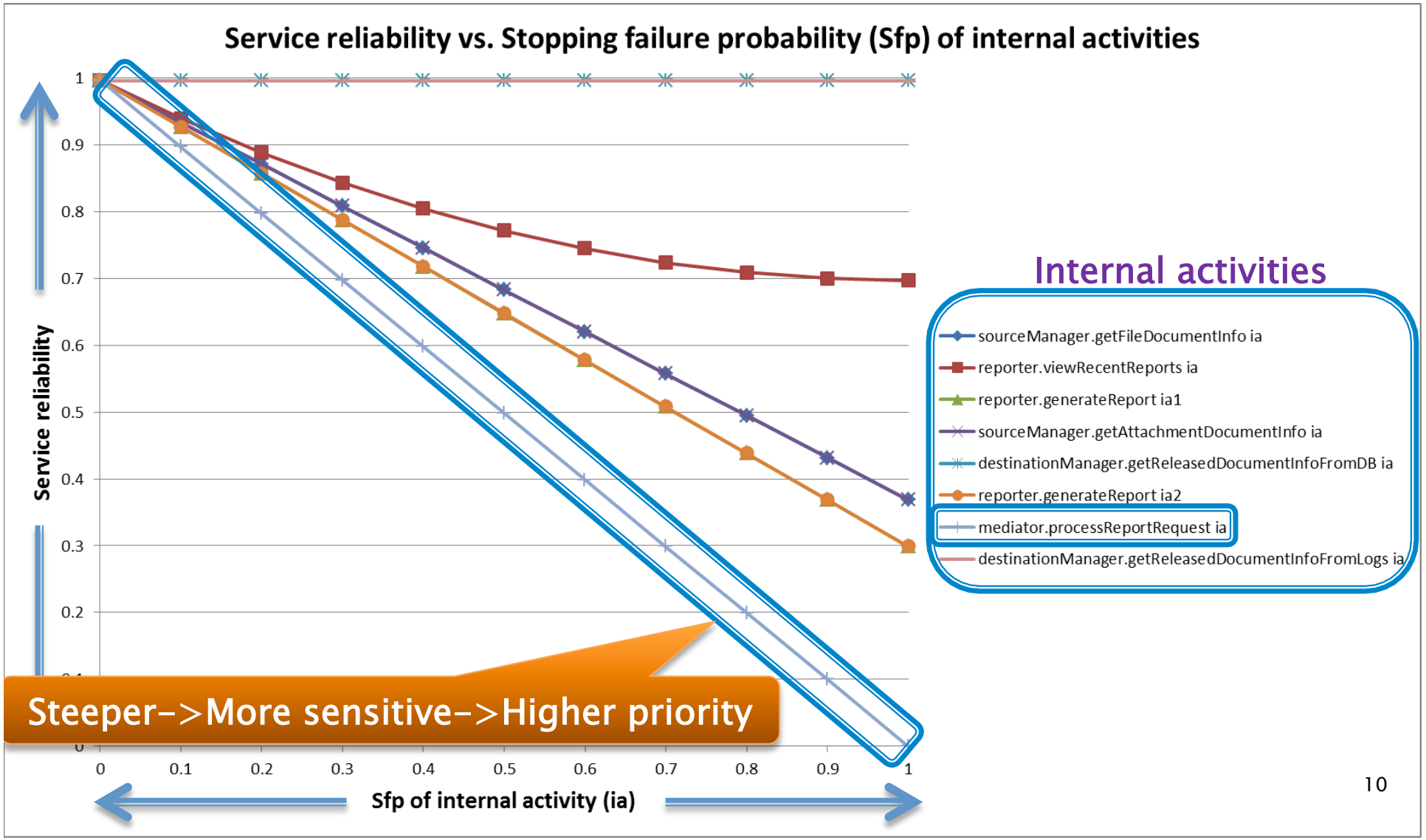
Usage Profile

User Interface

Assessment and Action



Sensitivity Analysis (Sample)



Conclusion

- **Reliability Modeling Tool**
  - Component based Model, Error propagation
  - Automatic
  - Design information
  - Sensitivity
- **Ongoing**
  - More general FT techniques
    - Active replication, Exception handling,…
  - Multiple Errors / Failure Modes / Interferences
  - Validation
    - Document management / scanning software
    - Fault-injection