

Long term goal: Predict Reliability of SW systems



Build
Controls Libraries
and SW components with quality warranties

System
Reliability
Model

Design:
Non functional
Requirements &
Threat Catalogue

Deploy and Run:
Incident History
& Metrics

Connect goals and methodologies across SDLC

- **Design:**
 - Dependability as attribute of the system architecture
 - We want to know how much dependability we get for the effort
- **Build:**
 - Reliability and Security as intentions of the development process
 - Minimize vulnerability potential by addressing threats also in SDLC
- **Run:**
 - Automation shall decrease the deployment costs
 - Run-time metrics are designed in the early stage of SDLC
 - We want to prove that the dependability is there

Risk based Controls/Safeguard Selection

- Designed and built-in dependability characteristics
 - Quantifiable
 - Respond to Threats -> Risks
- Danger of Risk based approach
 - Clear Governance and accountability shall prevent easy risk acceptance
 - SLA's need to be constructed from dependability characteristics
- Systemic risks and risk propagation
 - Highly coupled systems are reality
 - Patching current legacy systems together increases risks supra-linearly