Design and Implementation Oriented Validation of Survivable Systems


**Supporting Functional Assumptions**

- PKCS #11 Model

**DoD Assumptions**

- It can be shown that: Let PUB be the requirement of "successfully process a publish request".
- Let C be the preconditions.
- $E$ is the data flow of the publish is correct.
- $E_1$ = timeliness
- $E_2$ = integrity
- $E_3$ = confidentiality
- The requirement: PUB: $P(E|C) > p$

**Design Phase Validation**

1. **Step 1**: Formulate a precise statement of $R$.
2. **Step 2**: If $R$ is logically decomposable, decompose it iteratively.
3. **Step 3**: For every atomic requirement $R_i$.
4. **Step 4**: Build high-level description of System and its operational environment.
5. **Step 5**: Justify the modeling assumptions of Step 4.
6. **Step 6**: Construct a simulation model.
7. **Step 7**: Evaluation and comparing.

**Implementation Phase Validation**

**Survivable Publish Subscribe System**

**Data Flow**

**Infrastructure-level attacks**

**Gateways**

**Network**