EMV2 Errata

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Peter Feiler

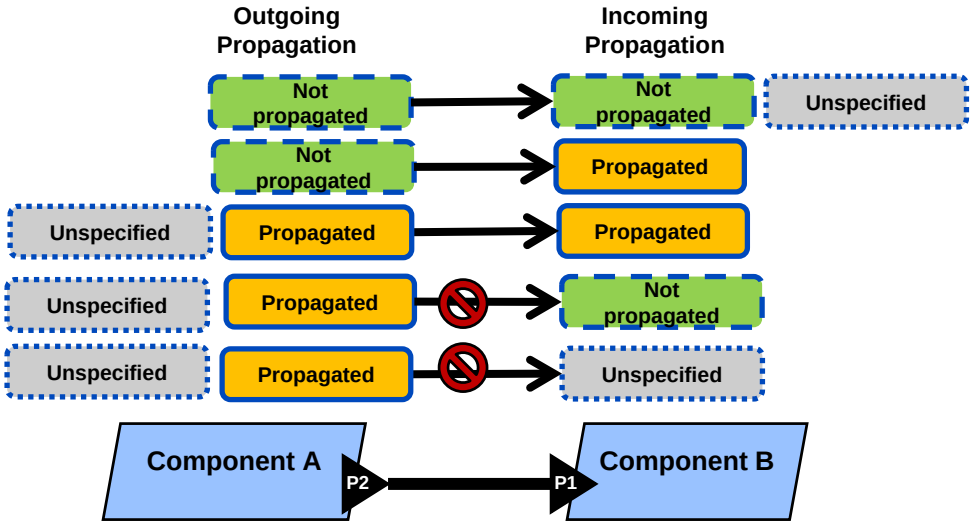
Jan 2017

Error Path Type Consistency Rule

Set of outgoing propagated error types contained in set of incoming error types

Set of incoming contained error types contained in set of outgoing contained types

Should we say anything if an error type is specified as part of a propagation or containment on one side but not on the other?



Logical expression issues

Binary exclusive or Operators

- Keyword OR: XOR semantics
- A1 XOR A2 XOR A3
  - Boolean logic interpretation: A1 = T A2 = T A3 = T => T
  - Intended interpretation: XOR (A1, A2, A3), i.e., one failure only

Event and state based condition evaluation

- Error events are occurring independently
  - Only one at a time can trigger a transition
  - Should not directly impact outgoing propagation condition
- Error propagations reflect error state
  - Evaluation of multiple is possible

Logical operators on propagations

Existing operators

- k **ormore** n: inclusive or starting with k subset
- k **orless** n: inclusive or up to k subset

Proposal: add k **of** n operator

- Any subset of size k failure
- 1 **of** (a1, a2, a3) exactly one failure
- Use case: triple redundant sensors
  - If one fails go to degraded mode
  - If 2 or more fail go to failstop mode

Support arrays

- 1 **ormore** (p1, p2, p3)
- 1 **ormore** (p[3])

Binding points: potentially unknown # of propagation sources

- Does conditional logic make sense on bindings