EMV2 Errata

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Peter Feiler

Oct 2016

Acceptable Operands for OrMore/OrLess

Current specification

- K **ormore**(trigger1, trigger2, .., trigger)
- Inclusive k of n
- Trigger ::= error event | incoming propagation

Proposal: allow condition expression

- 1 **ormore** (insensor1 **and** insensor2, failevent, overheatevent)
- Achievable with current syntax:
  - Separate statements, e.g., transitions, interpreted as inclusive or
    - Operational –[insensor1 **and** insensor2]-> FailStop;
    - Operational –[1 **ormore** (failevent, overheatevent)]-> FailStop;

Semantics of XOR operator

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

Proposal: 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

Other operators

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